Civitanova Marche, 27 novembre 2015

2° Workshop AIPSI del Ciclo Cyber Crime e Cyber Security

"I crimini informatici a danno di imprese, enti e liberi professionisti: come tutelare in modo efficace la sicurezza delle informazioni"

Il trend attuale degli attacchi digitali in Italia
I dieci comandamenti
per rendere più sicuro il proprio sistema informativo

Marco R.A. Bozzetti

CEO Malabo Srl

Ideatore e curatore OAI

Consiglio Direttivo e Communication Officer AIPSI

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

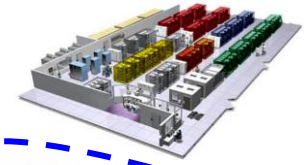
- **Primari obiettivi AIPSI**
  - diffondere la cultura e la sensibilizzazione per la sicurezza informatica agli utenti digitali,
  - offrire ai propri Soci qualificati servizi per la loro crescita professionale

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

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

Sicurezza vo cercando ….

Sistemi informativi aziendali e delle PA



DCS

Consumerizzazione

… + mobile

Ambiente lavoro

Internet

Internet delle cose

Ambiente personale

Servizi ICT in cloud e/o terziarizzati

La sicurezza ICT assoluta non esiste ed è sempre più complesso gestirla

VDS, PLC, A/D Conv.

Social network

Sicurezza digitale …
non solo un problema tecnico

- La sicurezza dell'ICT è un elemento chiave per:
  - garantire la continuità operativa dell'Azi
    - La Business continuity è un p ss
  - le informazioni e le risorse IC no un asset e come tali vanno protette
  - garantire la compli mative e certificazioni

La sicurezza dell'ICT va governata dal vertice dell'azienda/ente allineandola alle necessità del business

OAI, Osservatorio Attacchi Informatici in Italia

- ***Obiettivi iniziativa***
  - Fornire informazioni sulla reale situazione degli attacchi informatici in Italia
  - Contribuire alla creazione di una cultura della sicurezza informatica in Italia
  - Sensibilizzare i vertici delle aziende/enti sulla sicurezza informatica

- ***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***
  - Assoluta indipendenza anche dagli Sponsor (sponsorizzazioni solo per coprire, almeno parzialmente, i costi di realizzazione)
  - Stretto anonimato dei rispondenti al questionario on line via web
  - Collaborazione con numerose associazioni (Patrocinatori) per ampliare il bacino dei rispondenti e dei lettori

Rapporto OAI 2015

Scaricabile gratuitamente da:

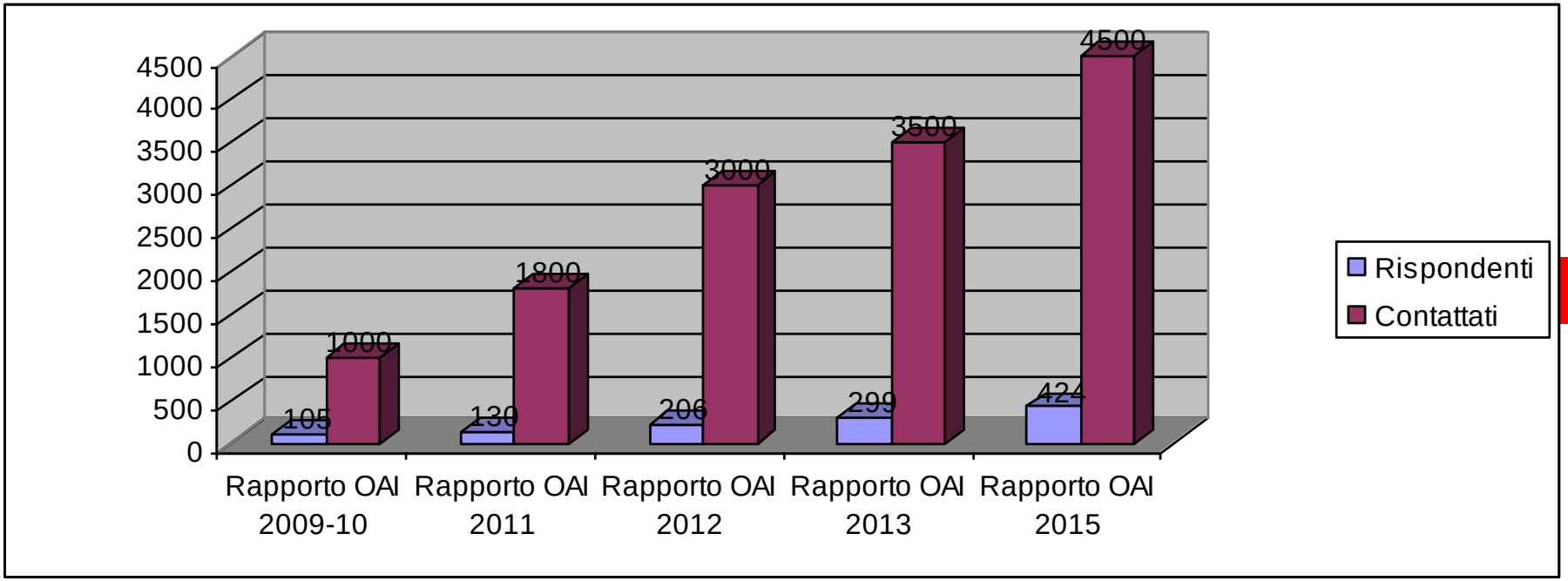
http://www.malaboadvisoring.it/index.php?option=com_content&view=article&id=61&Itemid=104

Sponsorizzazioni e patrocini OAI 2015

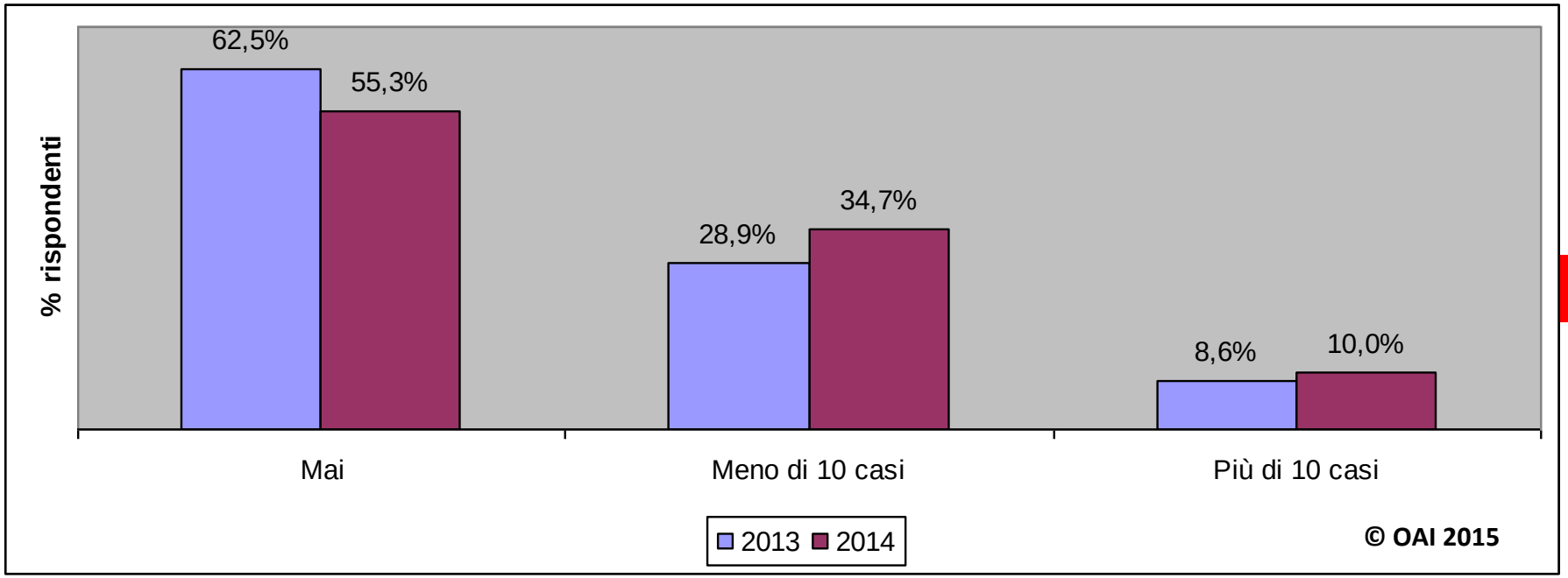
con la collaborazione di

Patrocinatori

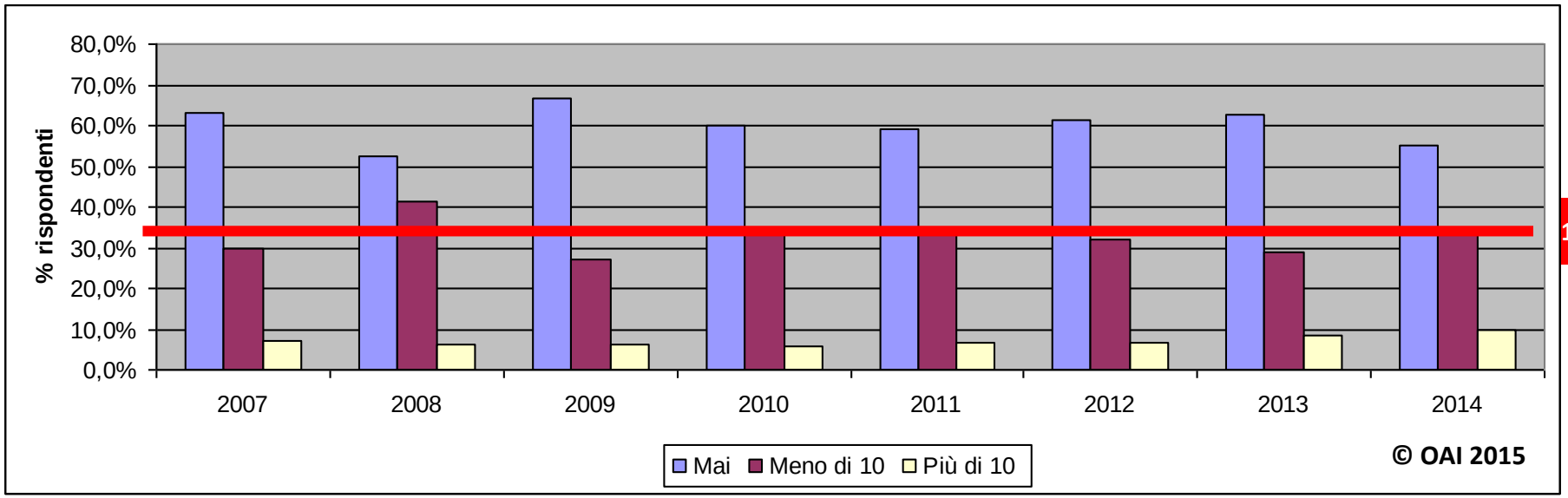
OAI 2009-2015: la crescita del numero di rispondenti



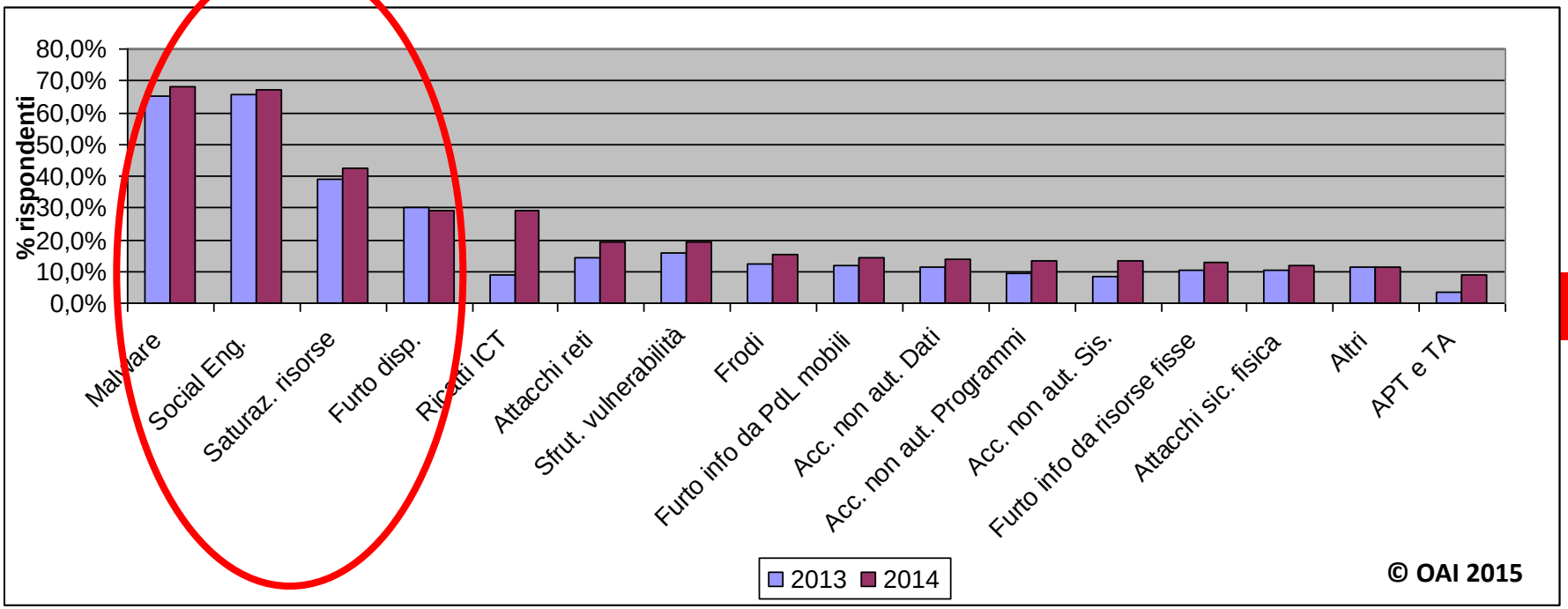
Attacchi rilevati nel 2013 e nel 2014



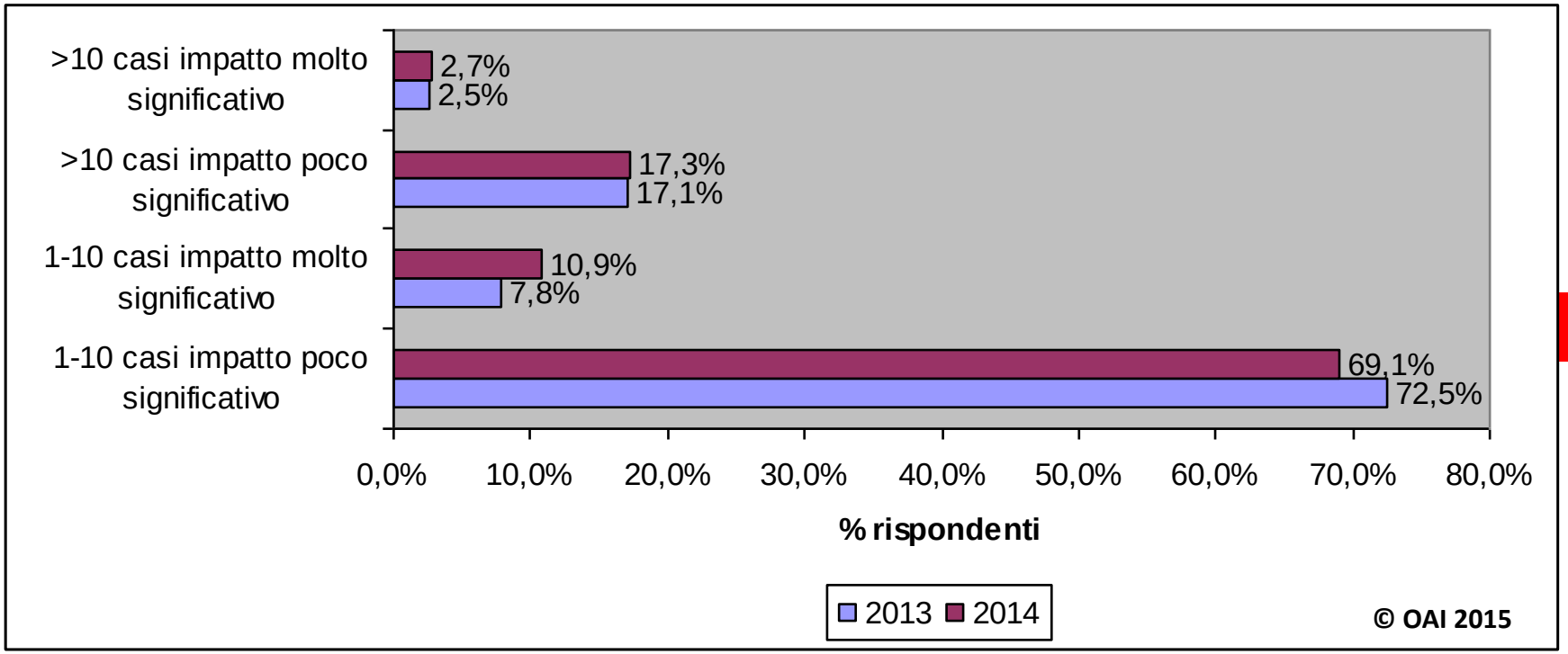
Attacchi rilevati dal 2007 nei vari Rapporti OAI



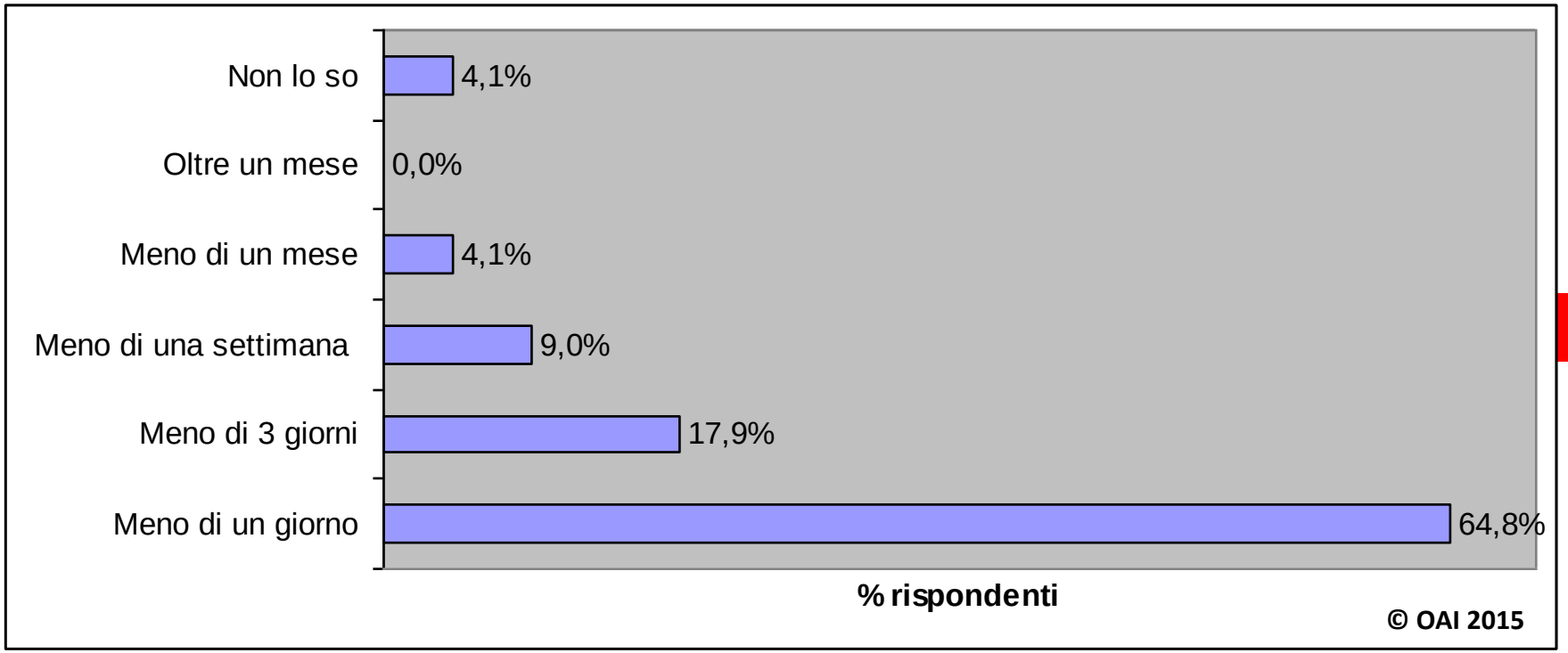
Diffusione tipologia attacchi subiti 2013 - 2014



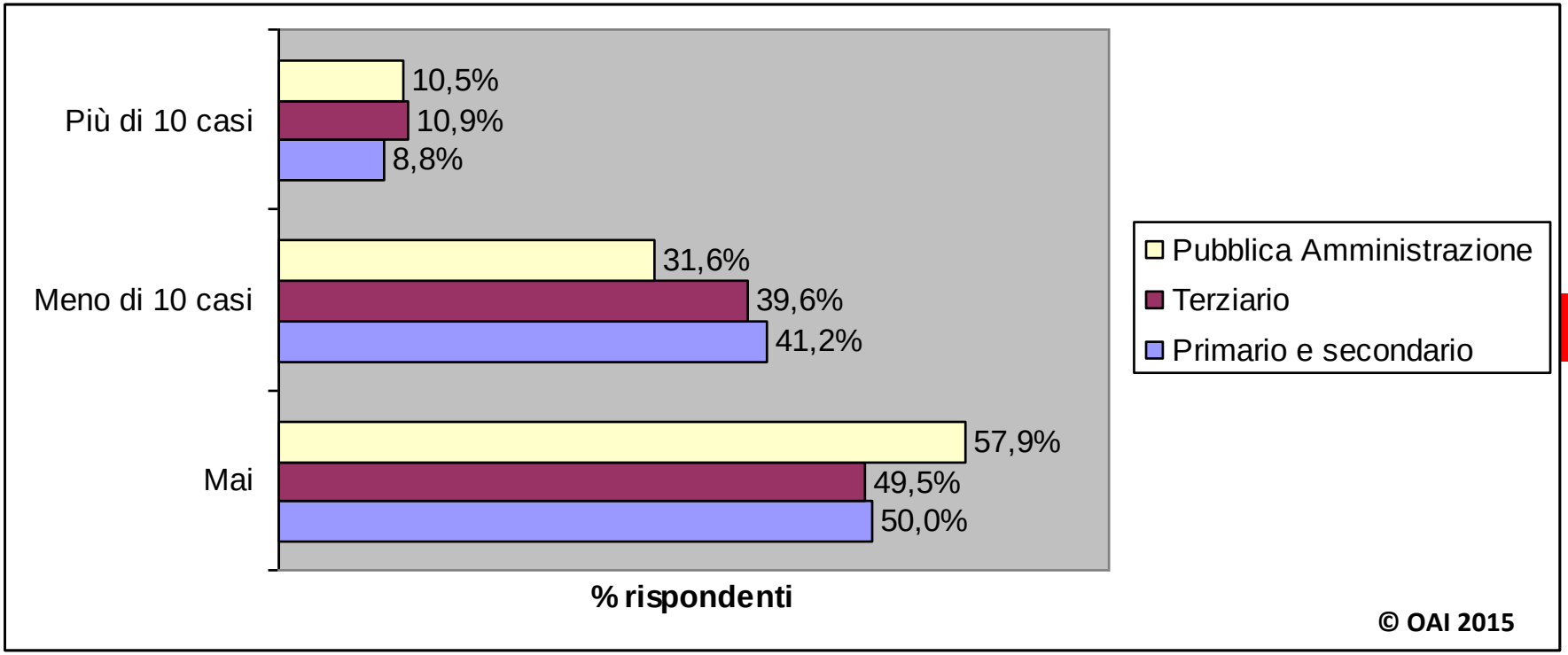
Impatto dell'attacco



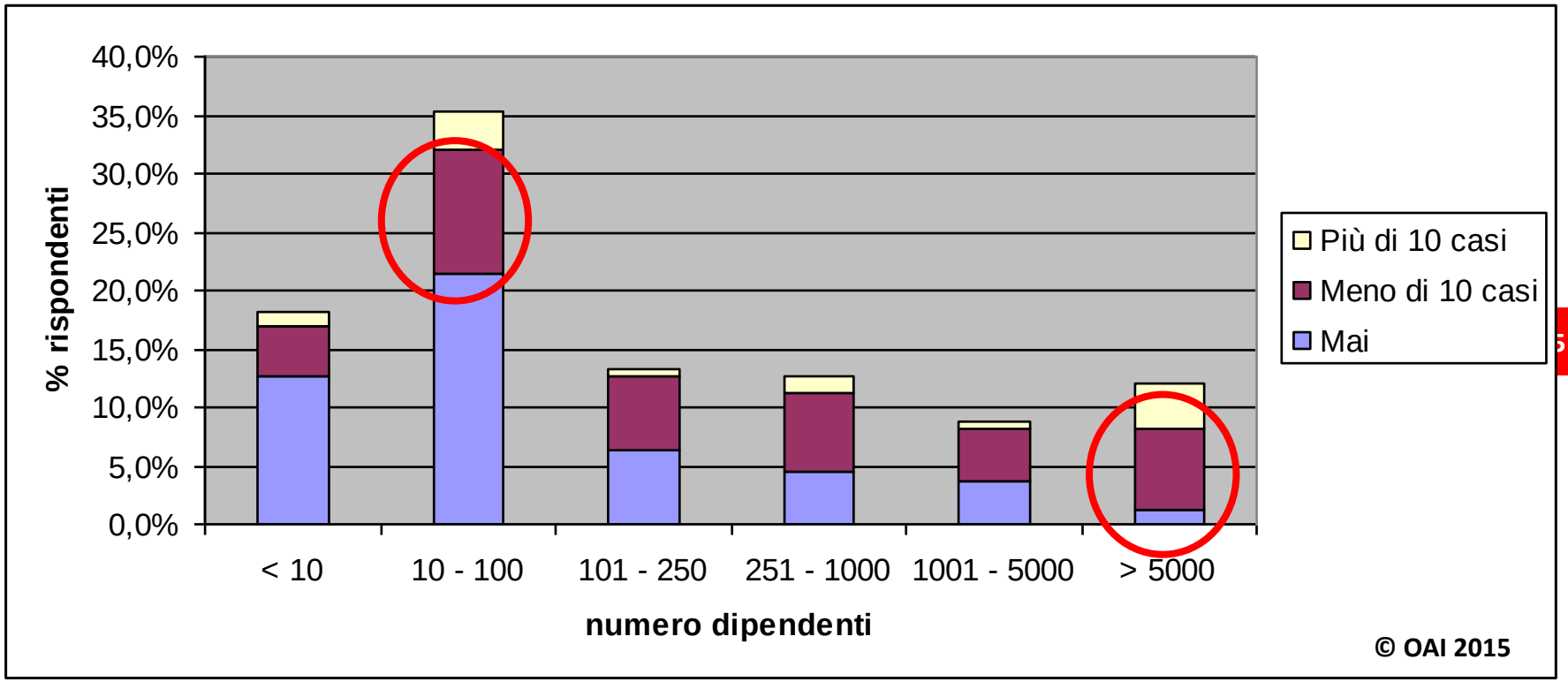
Tempi medi di ripristino dopo un attacco



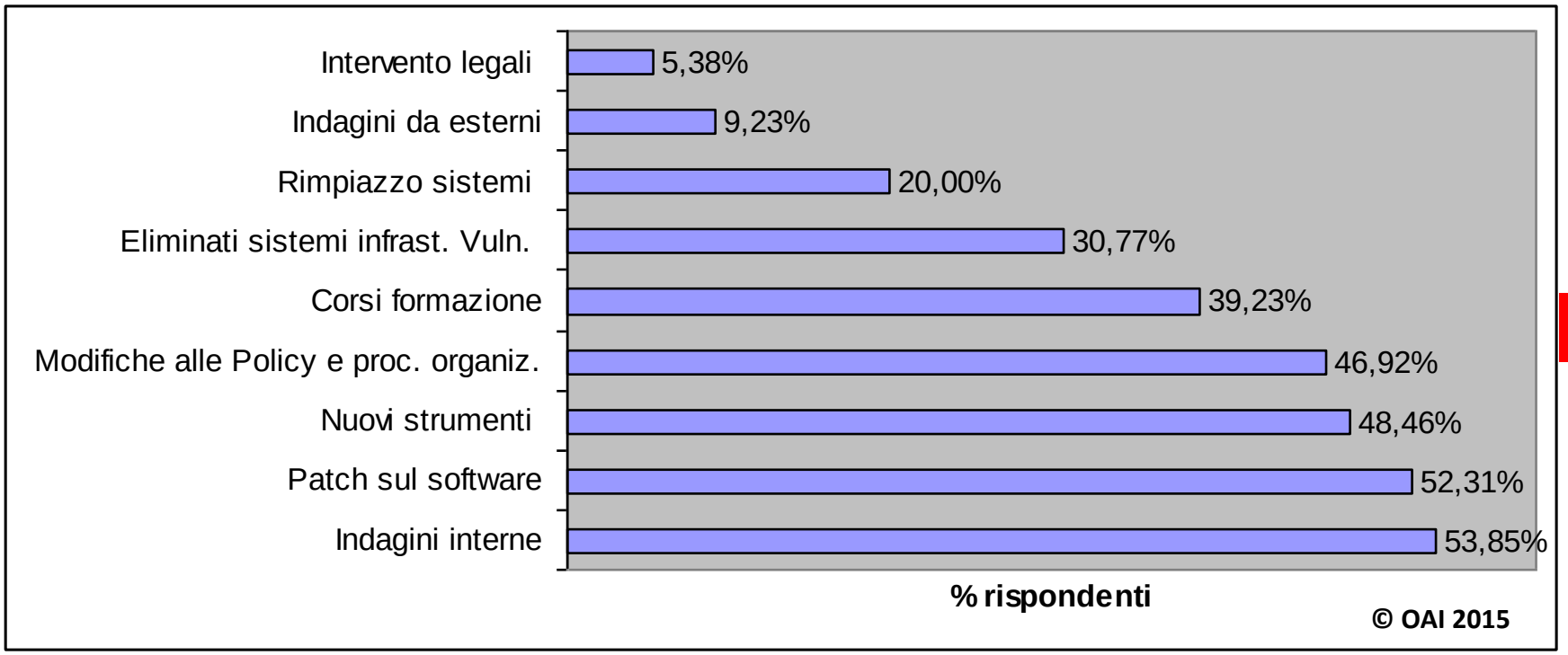
Attacchi 2014 per macro settore



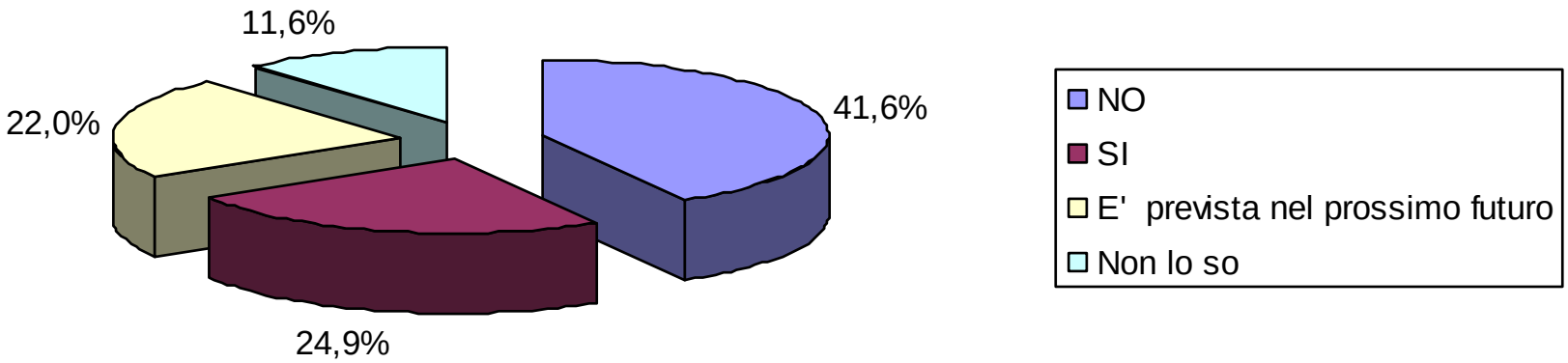
Attacchi 2014 per dimensione dell'azienda/ente



Azioni dopo un attacco



Effettuazione analisi dei rischi ICT



Richiesta conformità standard/best practice e certificazioni da OAI 2015

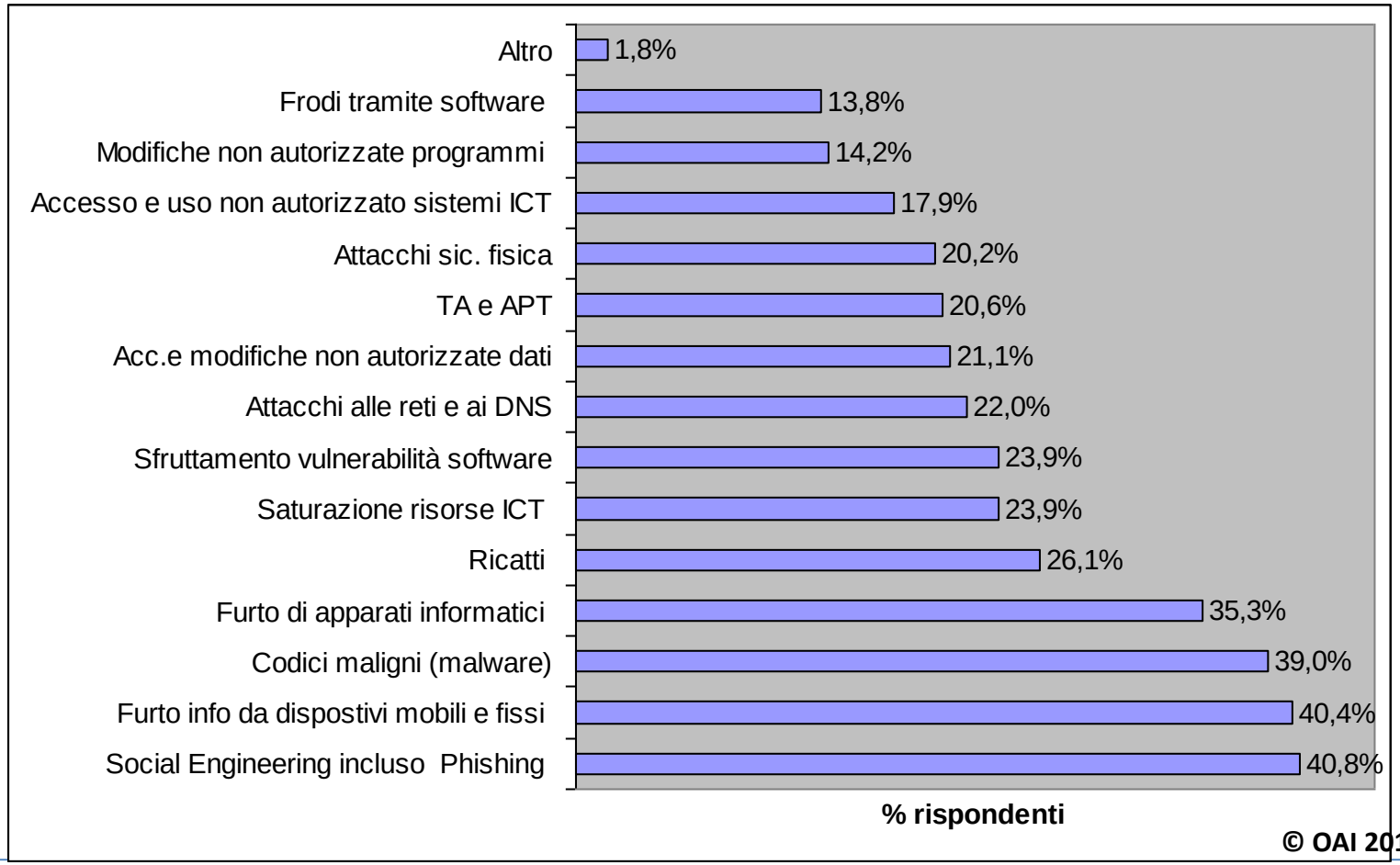
- *Famiglia ISO 27000*
  - **All'interno** → interesse/attuato, con o senza certificazioni: **62,4%**
  - **Dai Fornitori** → interesse/attuato, con o senza certificazioni: **37,5%**

- *ITIL e ISO 20000*
  - **All'interno** → interesse/attuato, con o senza certificazioni: **38,2%**
  - **Dai Fornitori** → interesse/attuato, con o senza certificazioni: **14,5%**

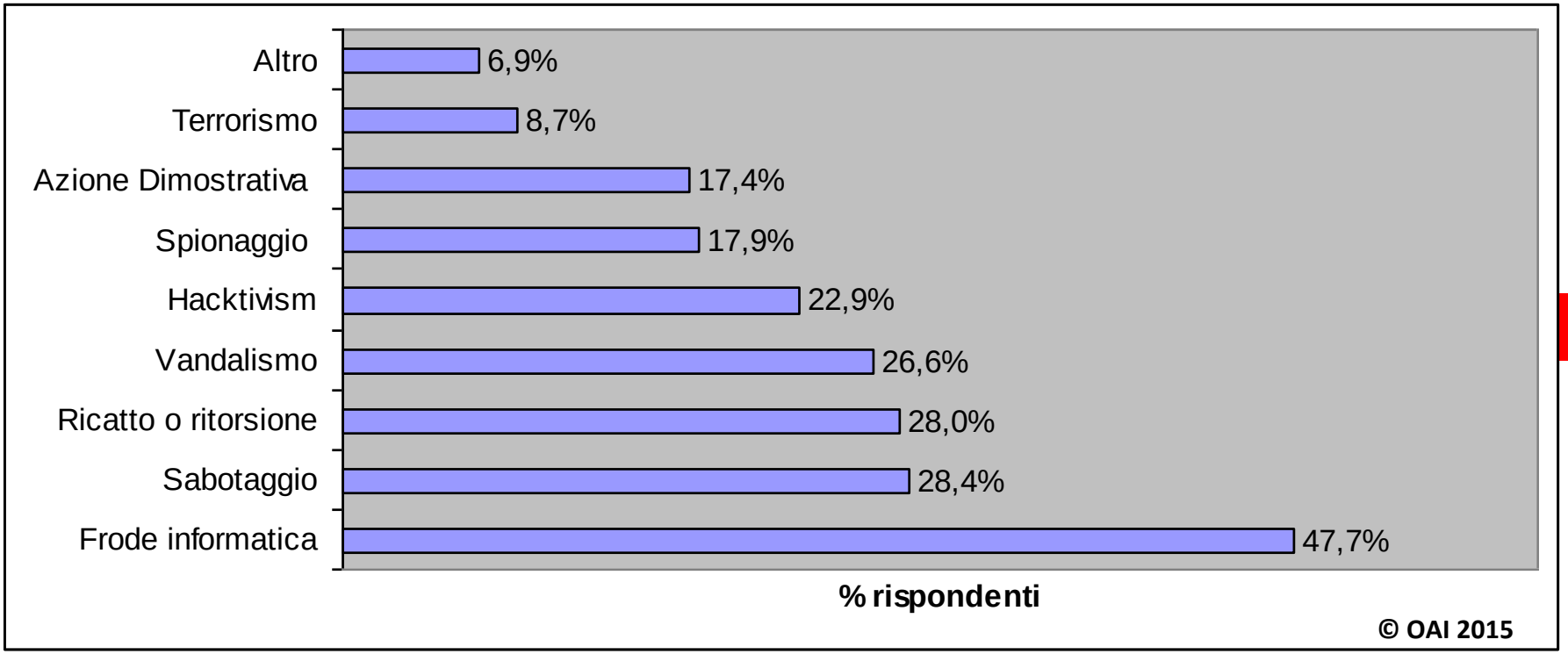
- *COBIT*
  - **All'interno** → interesse/attuato, con o senza certificazioni: **26,3%**
  - **Dai Fornitori** → interesse/attuato, con o senza certificazioni: **5,1%**

- *Certificazioni personali per la sicurezza ICT*
  - **All'interno** → interesse/attuato, con o senza certificazioni: **11,6%**
  - **Dai Fornitori** → interesse/attuato, con o senza certificazioni: **34,6%**

Attacchi maggiormente temuti nel futuro (risposte multiple)



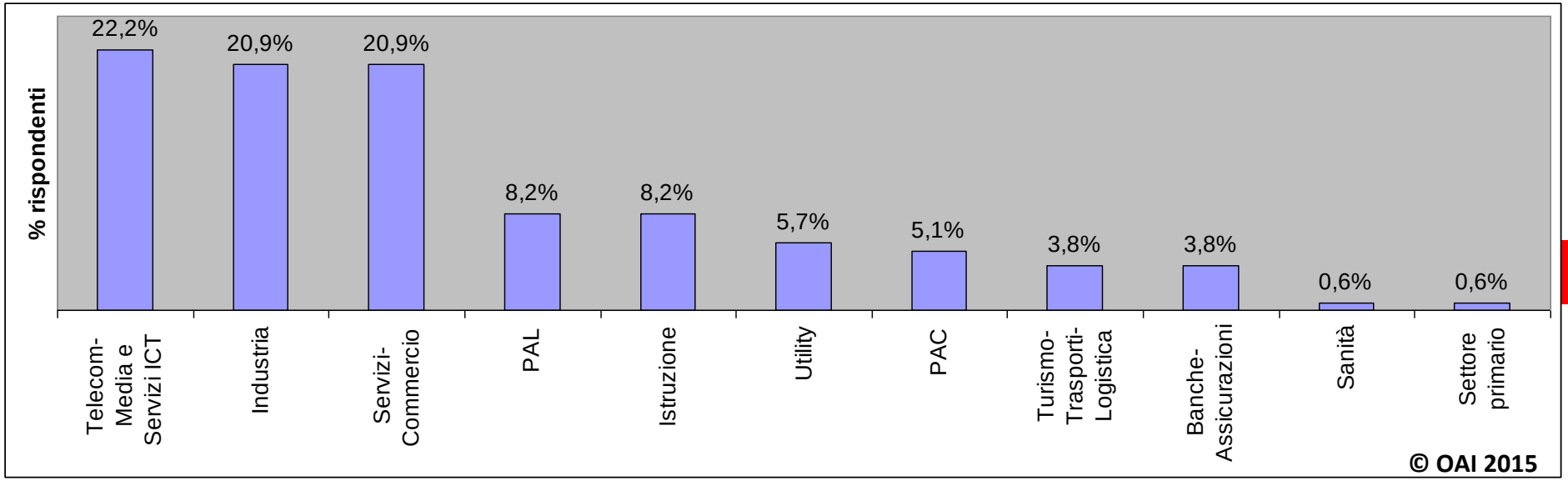
Possibili motivazioni per i futuri attacchi temuti (risposte multiple)



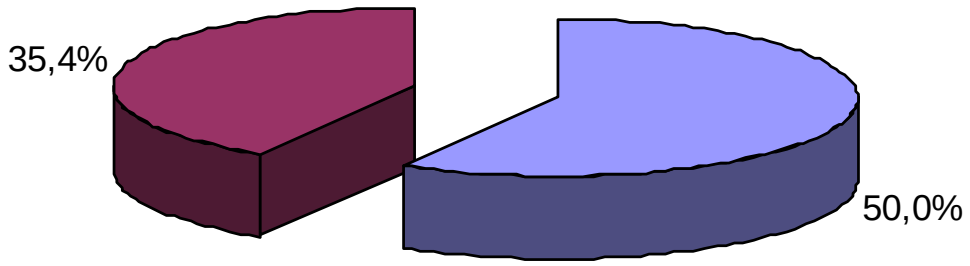
I trend futuri per gli attacchi

- Motivazioni:
  - vanno crescendo gli aspetti di protesta e politici, soprattutto per i paesi con governi dittatoriali o autoritari (Sud mediterraneo, Paesi arabi, ecc.)
  - Timori per una crescita di attacchi ICT di tipo terroristico (blocco e/o malfunzionamento infrastrutture critiche …)
  - Crescita attacchi per spionaggio (anche industriale)
  - Consolidamento crescita attacchi per frodi
- Il rischio di attacchi «massivi» ad un gran numero di aziende/enti anche piccoli (virus, ransomware, DDoS, ecc.)
- Crescita rischi e vulnerabilità nei sistemi “mobili”
- TA e APT, Advanced Persistent Threat
- Offuscamento (Obfuscation) delle attività dell’attaccante
- Proxy anonimi
- Sottrazione dati → focalizzazione sui contenuti
- Crescita dei siti “buoni” (affidabili) con collegamenti a siti maligni
- Disponibilità DIY Kit per la creazione di codici maligni e botnet sempre più facili da usare e poco costosi

Settore merceologico di appartenenza rispondenti

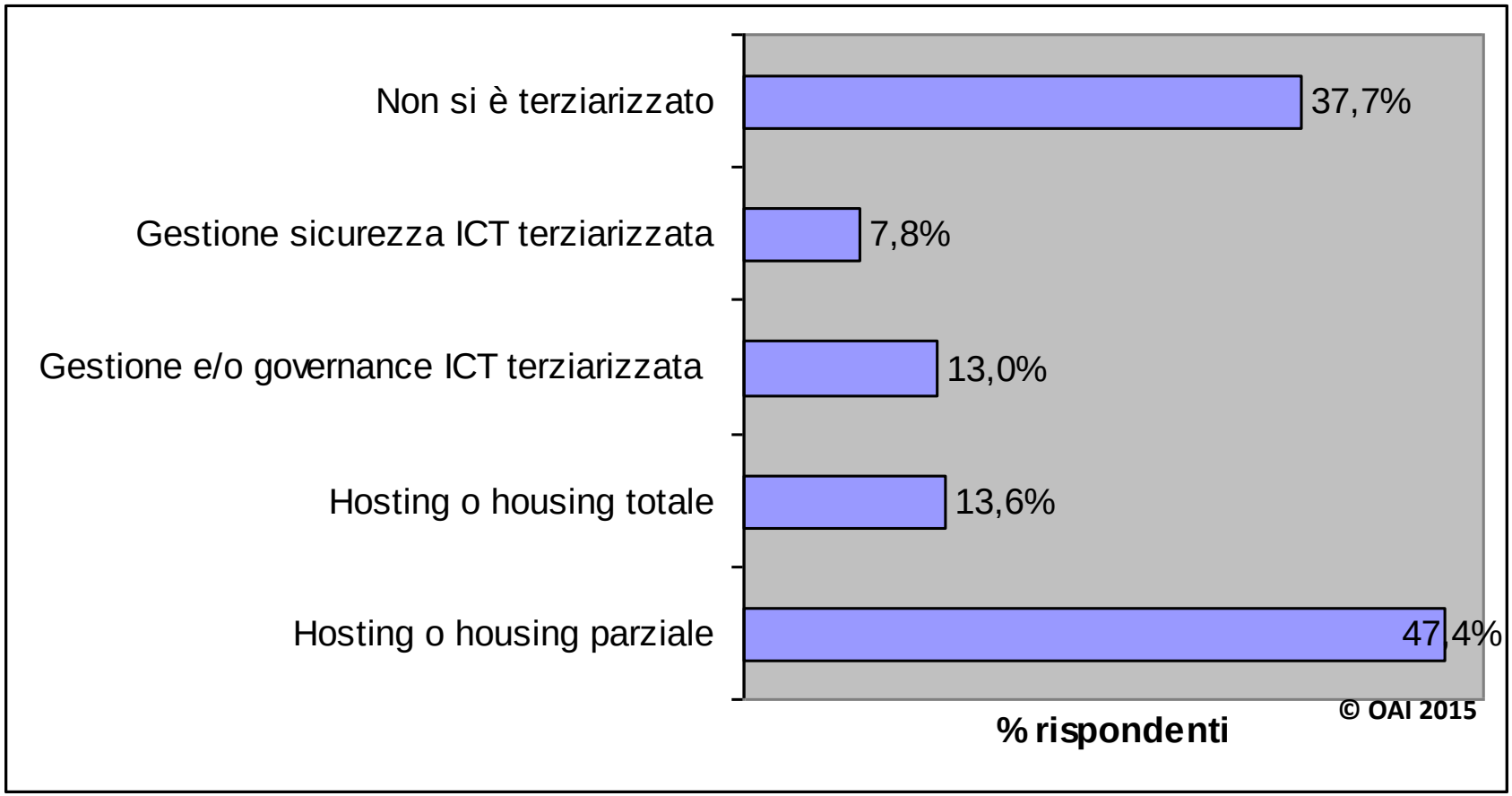


Alta affidabilità del sistema informatico rispondenti



- Architettura alta affidabilità (> 99,9%)
- Piano Business Continuity per ICT attivo

Uso terziarizzazione rispondenti (risposte multiple)



Come proteggersi ?

La sicurezza globale ICT

Sicurezza e budget ICT

- La sicurezza ICT rappresenta un **costo "continuo"** nel budget ICT → sistematica riduzione → aggravata dalla crisi

- Al vertice aziendale occorre presentare proposte di progetti e di spesa **in termini di business**, non tecnici
  - Il costo della sicurezza deve essere paragonato al costo della "**non sicurezza**", → Analisi del Rischio
  - I costi assicurativi sul rischio residuo diminuiscono al crescere del livello di sicurezza in atto
  - Con una visione a medio lungo termine ma con risultati entro l'anno
  - Interventi ben bilanciati e che tengano conto degli aspetti organizzativi

- Una debole e non misurabile sicurezza ICT
  - può far incorrere in sanzioni amministrative e/o **penali**: Legge 196 sulla privacy, Legge 231 sulla Governance,IAS…
  - **preclude al finanziamento** dalle Banche: Basilea 2-3, IAS…
  - non si possono produrre e vendere prodotti e servizi, oltre a non poter essere quotati in determinate Borse: IAS, SOX, HPPI...

Le misure tecniche

- 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.

- **Analisi e gestione dei rischi** sistematiche

- 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”

Le misure organizzative

- Non sono burocrazia
- Non sono solo per le grandi strutture
- Sono necessarie anche per la conformità a numerose norme e leggi nazionali ed internazionali
- Includono:
  - Chiara e pubblica definizione di **ruoli** e **competenze**
    - organigramma
    - separazione dei ruoli (**SoD, Separation of Duties**) → matrici RACI
  - Definizione delle **Policy** e delle relative **procedure organizzative**
    - Definizione dei controlli e di come attuarli
  - Selezione e controllo del personale e dell'uso dell'ICT
    - Auditing
    - Analisi dei log degli operatori e degli utenti ICT
  - Radiazione dei sistemi obsoleti
  - Sensibilizzazione, formazione, addestramento degli utenti e degli operatori

L’effettiva sicurezza ICT dipende da come viene gestita

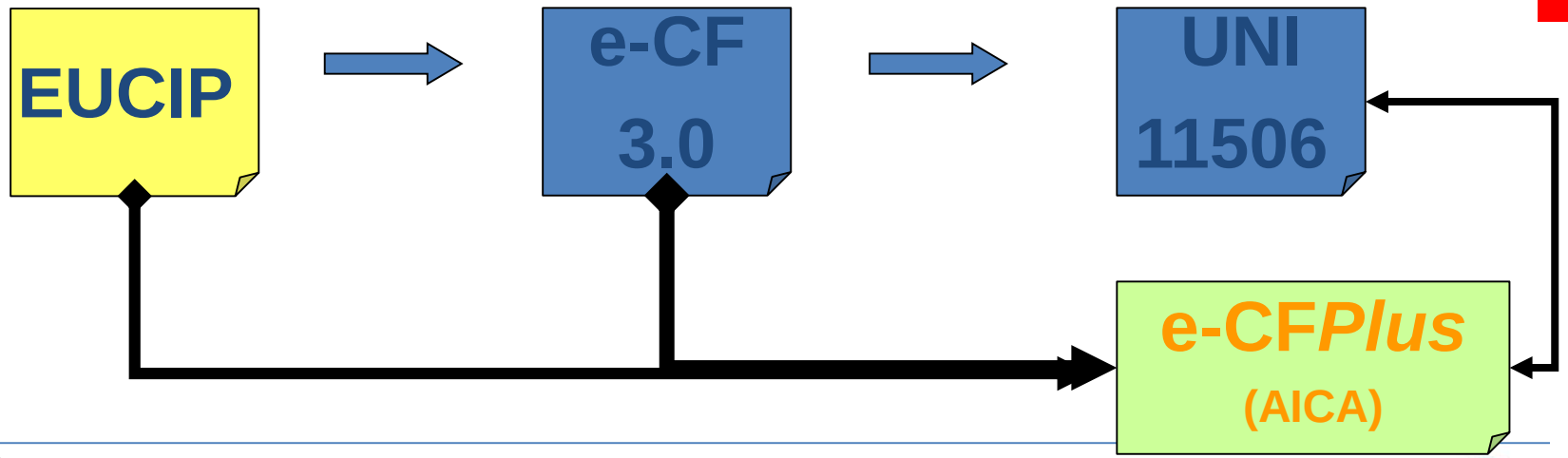
- Sia dal punto di vista **tecnico**
  - Può essere terziarizzata
- Sia dal punto di vista **organizzativo** e del **personale**
  - Deve essere gestita internamente
  - Forte commitment dal vertice aziendale
- Fondamentale avere strumenti di misura e controllo, usati sistematicamente
- Fare riferimento agli standard ed alle best practice consolidate: ISO 27000, Cobit 4.1- DS5 , Itil v.3, ecc.

Da professionista a *Professionista Certificato*

- D. Lgs. 16 gennaio 2013, n. 13
  - 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



10 considerazioni… pragmatiche e finali

1. La sicurezza assoluta non esiste
2. La Legge di Murphy è sempre vera, prima o poi qualche guaio arriva: bisogna essere preparati al ripristino
3. Il peggior nemico: la “falsa” sicurezza
4. La sicurezza è un processo continuo, sia per la parte tecnica che per la parte organizzativa
5. La sicurezza “globale” deve essere calata nello specifico contesto dell’Azienda/Ente: i suoi processi, i suoi sistemi, la sua organizzazione, la sua cultura
6. Per la legge, la forma è sostanza: non solo bisogna fare, ma anche documentare quello che si è fatto → compliance normative vigenti: privacy, safety, quality, ecc.
7. Qualunque siano le soluzioni e le modalità di intervento prescelte, è sempre il top management che deve dare un forte commitment, che deve guidare i fornitori, che deve dare il buon esempio
8. Prevenire, prevenire, prevenire: ma per far questo occorre misurare sistematicamente
9. La velocità e la complessità degli attuali attacchi è tale che i processi di gestione della sicurezza devono essere automatizzati
10. La sicurezza ICT è come una catena: tanto sicura quanto il suo anello più debole. Essa deve quindi essere “ben bilanciata” tra le varie misure e strumenti

OAI 2016: prossimi passi …

- Sono in corso tutte le iniziative per il prossimo **Rapporto 2016**
- **Molte novità nella nuova edizione**
- Chi fosse interessato a sponsorizzarlo è pregato di contattarmi:
  - marco.bozzetti@malaboadvisoring.it
  - m.bozzetti@aipsi.org
- A gennaio 2016 **compilate on line il Questionario 2016** !!!

Riferimenti

www.aipsi.org

www.issa.org

www.malaboadvisoring.it

Marco Rodolfo Alessandro Bozzetti

Attività professionale

- **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
- ***Certificazioni***: ITIL v3, Eucip Livello Professionale Security Adviser

Associazioni

- *FTI, Forum delle Tecnologie dell'Informazione (fondatore)*
- *ClubTI di Milano (Past President)*
- *FidaInform, Federazione Italiana delle Associazioni Professionali di Information Management (Past President)*
- *AIPSI-ISSA, Consiglio Direttivo – Comms Officer*

Principali iniziative

- *EITO, European Information Technology Observatory (Co-ideatore e Chief Scientist)*
- *EAC, Enterprise Architecture Conference*
- *OAI, Osservatorio Attacchi Informatici in Italia*

OsservatorIO AttacchInformatici

aipsi ASSOCIAZIONE ITALIANA PROFESSIONISTI SICUREZZA INFORMATICA

malabo ICT Advisory

Malabo Srl

- Malabo Srl, fondata nel 2001, opera nell'ambito della consulenza e dell'erogazione di servizi ICT per Clienti sia lato domanda sia lato offerta

www.malaboadvisoring.it

- Forte competenza e specializzazione sulle architetture e sulla sicurezza ICT, ivi inclusa l'analisi e la gestione dei rischi
    - Dal 2009 realizza OAI, Osservatorio Attacchi Informatici in Italia

- Caratteristiche di ogni intervento:
    - creare valore misurabile, trasparenza ed indipendenza decisionale, trasferimento di know-how;
    - Contestualizzazione e personalizzazione sulla specifica realtà del Cliente, in maniera veloce ed economica grazie all'esperienza dei Partner Malabo

Malabo Srl: la consulenza

- **Consulenza tecnica**
  - Sicurezza ICT
  - Analisi e gestione dei rischi
  - Razionalizzazione Sistema Informatico (riduzione costi e miglioramento livelli di servizio)
  - Piano evoluzione Sistema Informatico , terziarizzazioni e cloud
  - ICT Enterprise Architecture
  - Sicurezza informatica ed analisi dei rischi
  - Supporto e collaborazione in grandi progetti
  - Supporto al CIO, CTO, CSO, CISO
- **Consulenza manageriale ed organizzativa**
  - Governance ICT allineata alla governance aziendale
  - Riorganizzazione struttura, responsabilità e processi ICT
  - Automazione e razionalizzazione processi ICT (Cobit, ITIL, NIST, ecc.)
  - Compliance (privacy, safety, ecc.) e supporto alle certificazioni
  - Analisi del valore dell'ICT per l'azienda/ente
  - Supporto marketing e strategico (lato offerta ICT)
  - Analisi trend tecnologie e mercati
  - Innovazione per e con l'ICT

Malabo Srl: i Servizi

- Consentono di facilitare l'attuazione degli interventi consulenziali e consentono al Cliente di continuare autonomamente la gestione di quanto effettuato con l'intervento consulenziale
- **I servizi on line**
  - **SLA Watch** per il monitoraggio ed il controllo delle prestazioni delle risorse ICT
    - → www.slawatch.com

  - **GOSI,** per l'automazione dei principali processi ICT e la governanceoperativa del Sistema Informatico
  - **RIESKO** per l'analisi e la gestione dei rischi

  - **ACR ICT** per l'analisi delle competenze e dei ruoli del personale ICT sulla base degli standard eCF ed UNI 11506
  - **ANVA**, per l'analisi del valore dell'ICT
  - **DPS/DVR Kit** per l'analisi e la stesura dei documenti per la privacy e la safety