smau

MILANO 21-22-23 OTTOBRE 2015

Le maggiori criticità sugli attacchi informatici in Italia e come difendersi

Marco R.A. Bozzetti

CEO Malabo Srl
Ideatore e curatore OAI
Consiglio Direttivo e Communication Officer AIPSI

fieramilanocity

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.

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 2015

Scaricabile gratuitamente da:

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

Sponsorizzazioni e patrocini OAI 2015

AICA
aipsi ASSOCIAZIONE ITALIANA PROFESSIONISTI SICUREZZA INFORMATICA
BUSINESS-e SINCE 2000 BE your Security Company
hp
Riesko Manage your risks
sernet GROUP
Technology Estate
TREND MICRO

con la collaborazione di

polizia delle comunicazioni

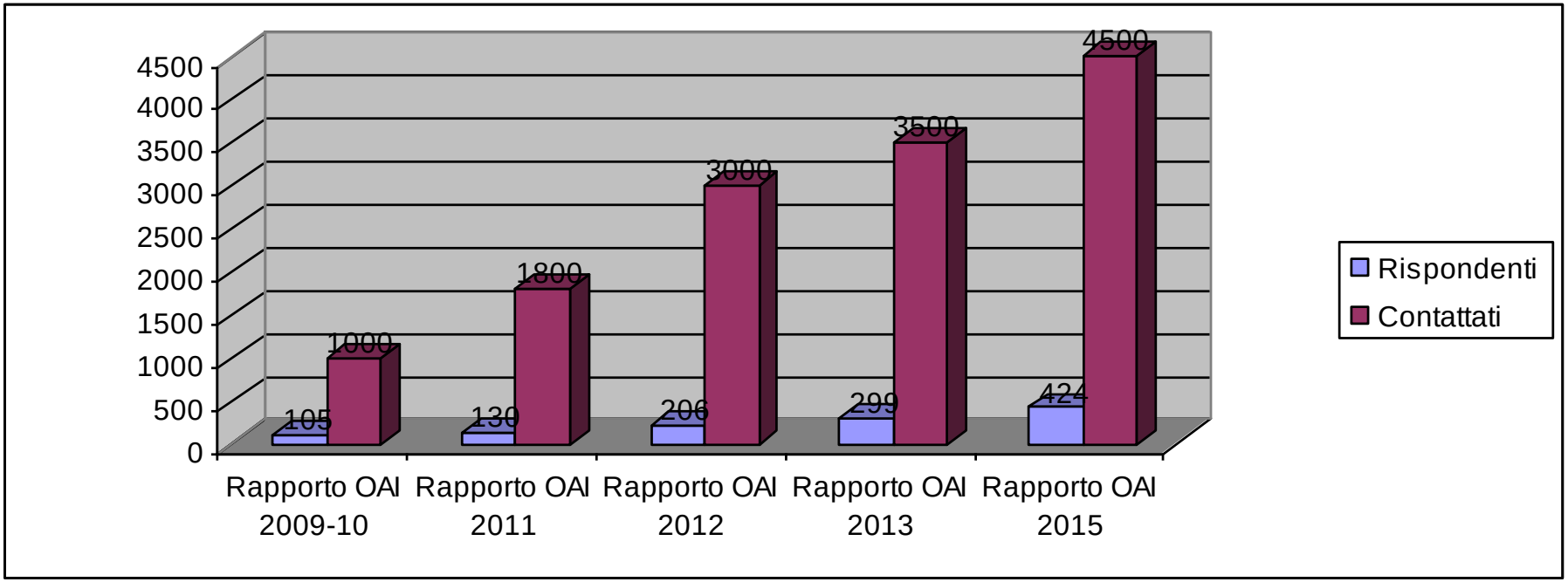
Patrocinatori

AICA
aipsi ASSOCIAZIONE ITALIANA PROFESSIONISTI SICUREZZA INFORMATICA
ASSINTEL ASSOCIAZIONE NAZIONALE IMPRESE ICT
ASSOLOMBARDA
ASSI Associazione Utilizzatori Sistemi e tecnologie dell'Informazione
Club Dirigenti di Informatica
CDTI
ti
ClubTI Club per le tecnologie dell'informazione
CTIer 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

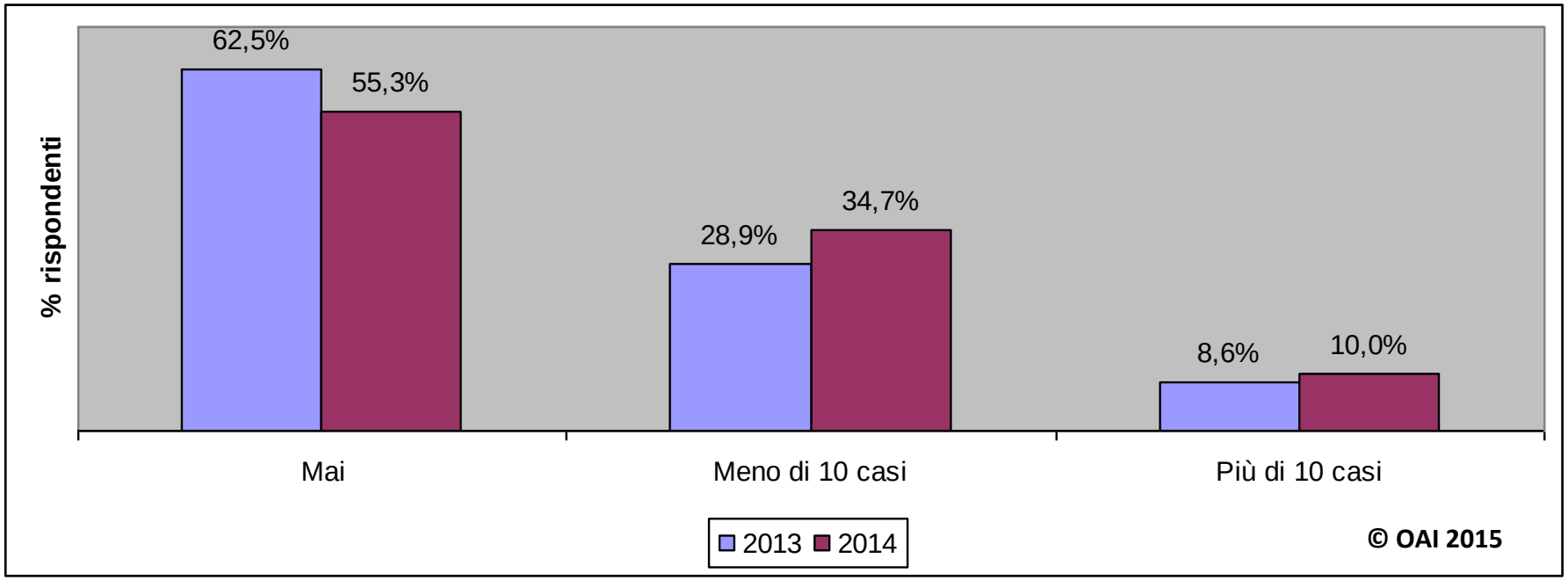
oai OsservatorIO AttacchInformatici

fieramilanocity

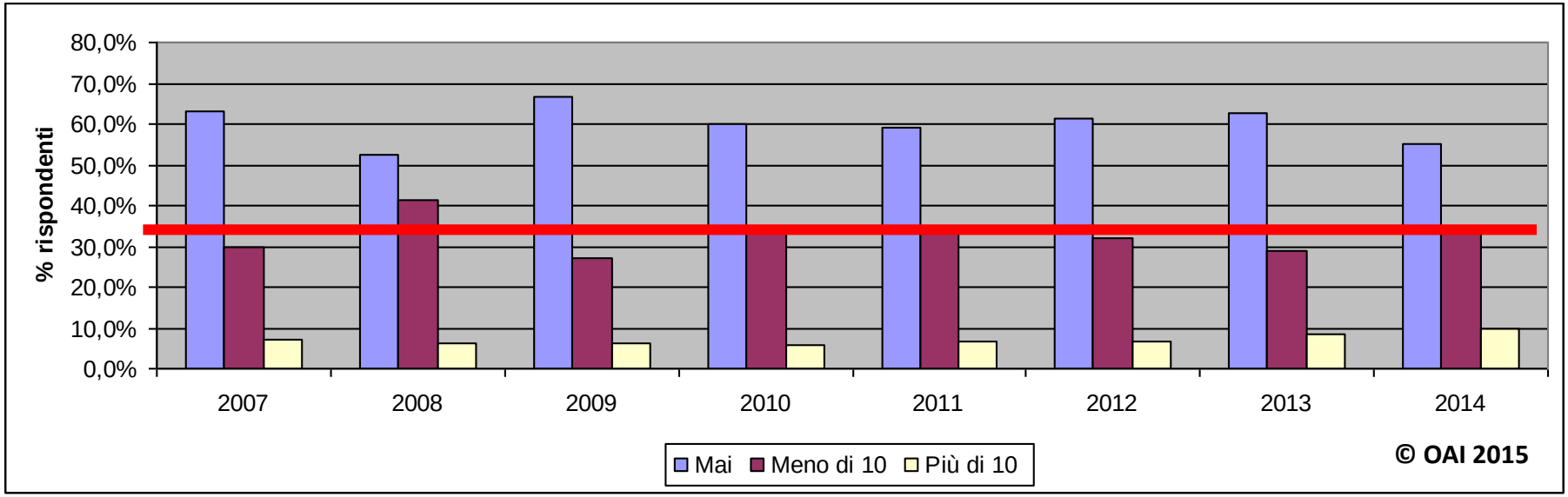
OAI 2009-2015: la crescita del numero di rispondenti



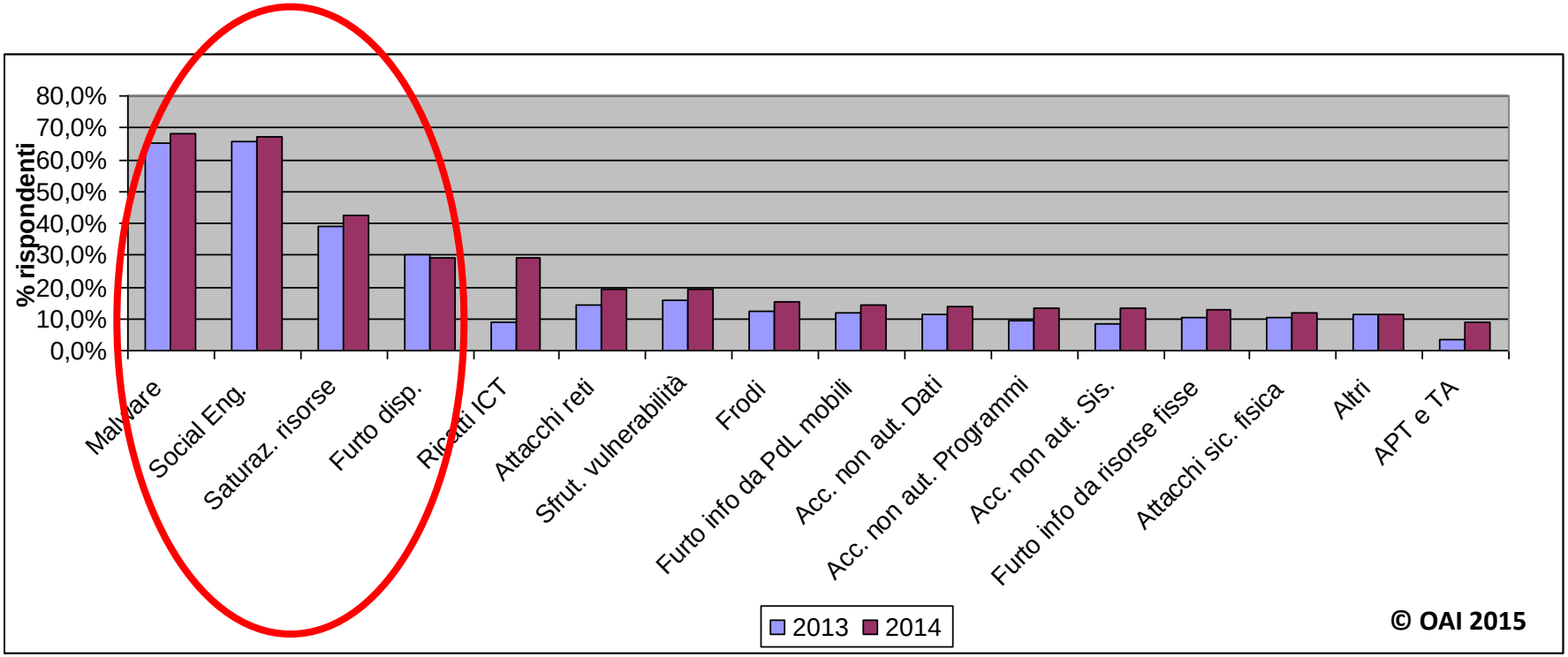
Attacchi rilevati nel 2013 e nel 2014



Attacchi rilevati dal 2007 nei vari Rapporti OAI



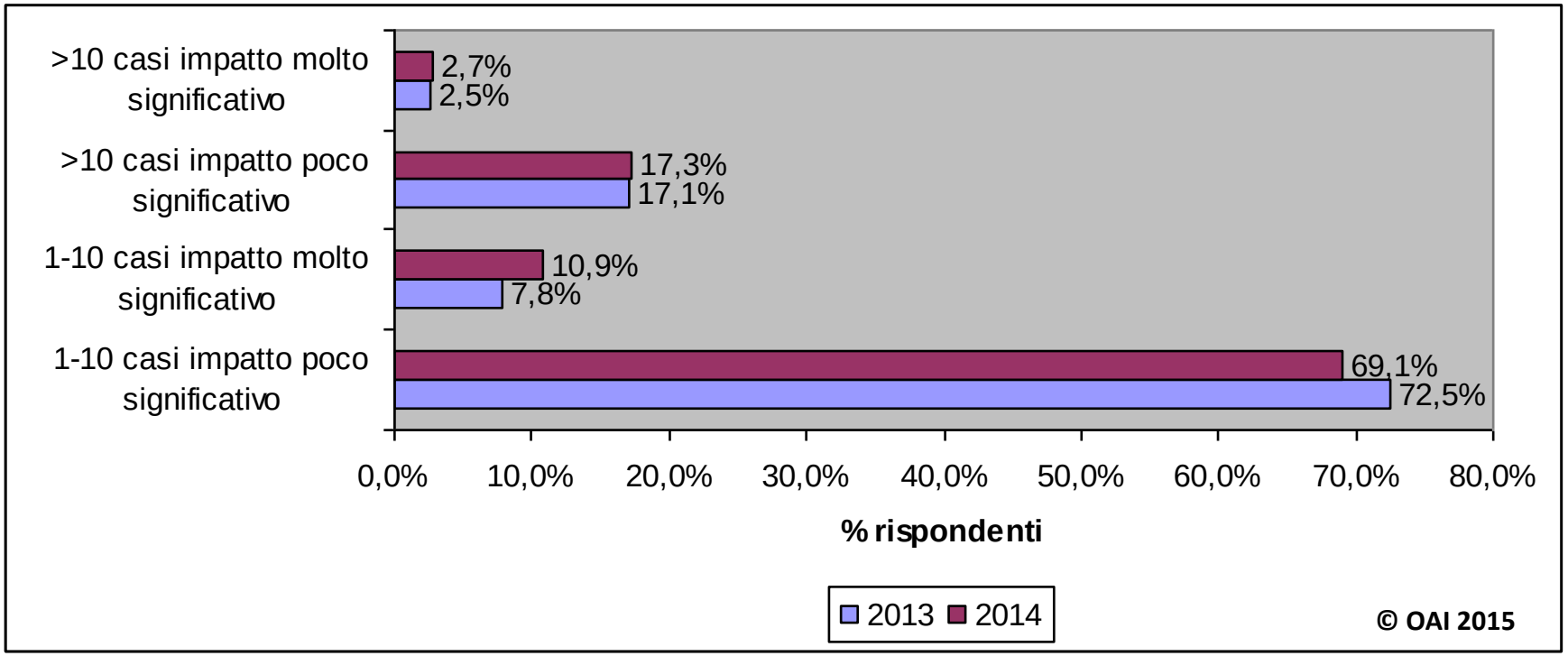
Diffusione tipologia attacchi subiti 2013 - 2014



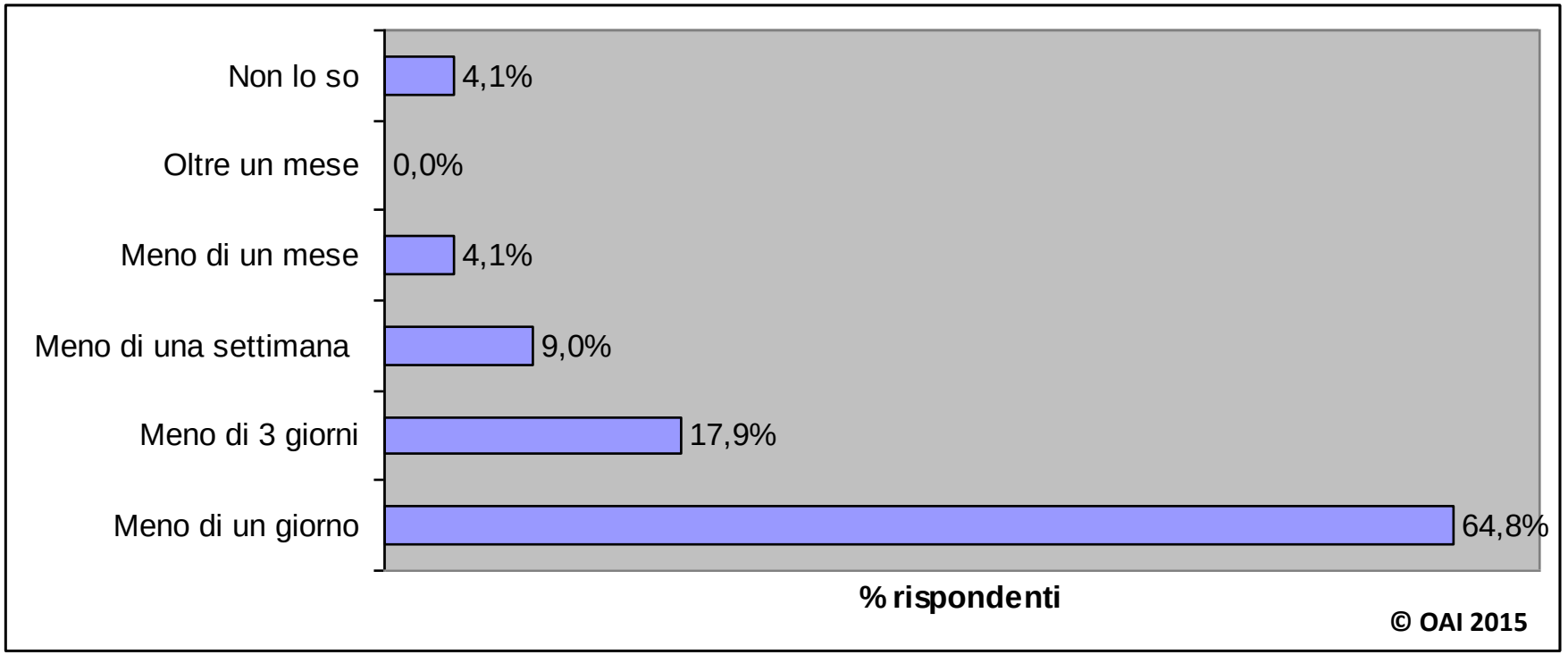
Ordinamento attacchi per variazione % tra 2014 e 2013

Classifica	Tipologia attacchi	2013	2014	Variazione
5	Ricatti ICT	8,7%	28,9%	20,2%
16	APT e TA	3,3%	8,9%	5,6%
13	Acc. non aut. Sis.	8,3%	13,4%	5,1%
7	Attacchi reti	14,5%	19,2%	4,7%
10	Acc. non aut. Programmi	9,3%	13,4%	4,2%
3	Saturaz. risorse	38,8%	42,5%	3,7%
6	Sfrut. vulnerabilità	15,8%	19,1%	3,3%
11	Acc. non aut. Dati	11,2%	14,0%	2,8%
2	Malware	65,1%	67,9%	2,8%
8	Frodi	12,4%	15,1%	2,8%
9	Furto info da PdL mobili	11,9%	14,2%	2,3%
12	Furto info da risorse fisse	10,5%	12,7%	2,3%
1	Social Eng.	65,8%	67,1%	1,4%
14	Attacchi sic. fisica	10,4%	11,8%	1,4%
15	Altri	11,4%	11,5%	0,1%
4	Furto disp.	30,3%	29,2%	-1,1%

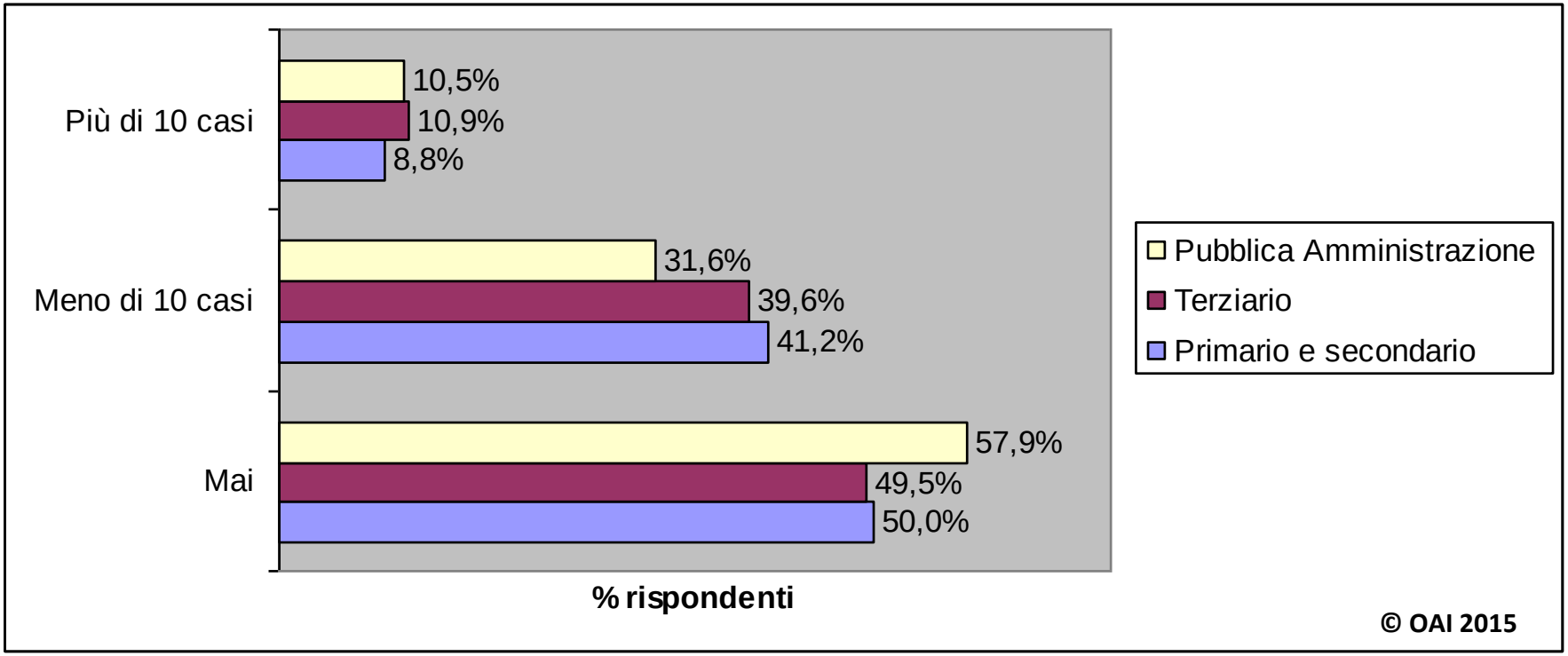
Impatto dell'attacco



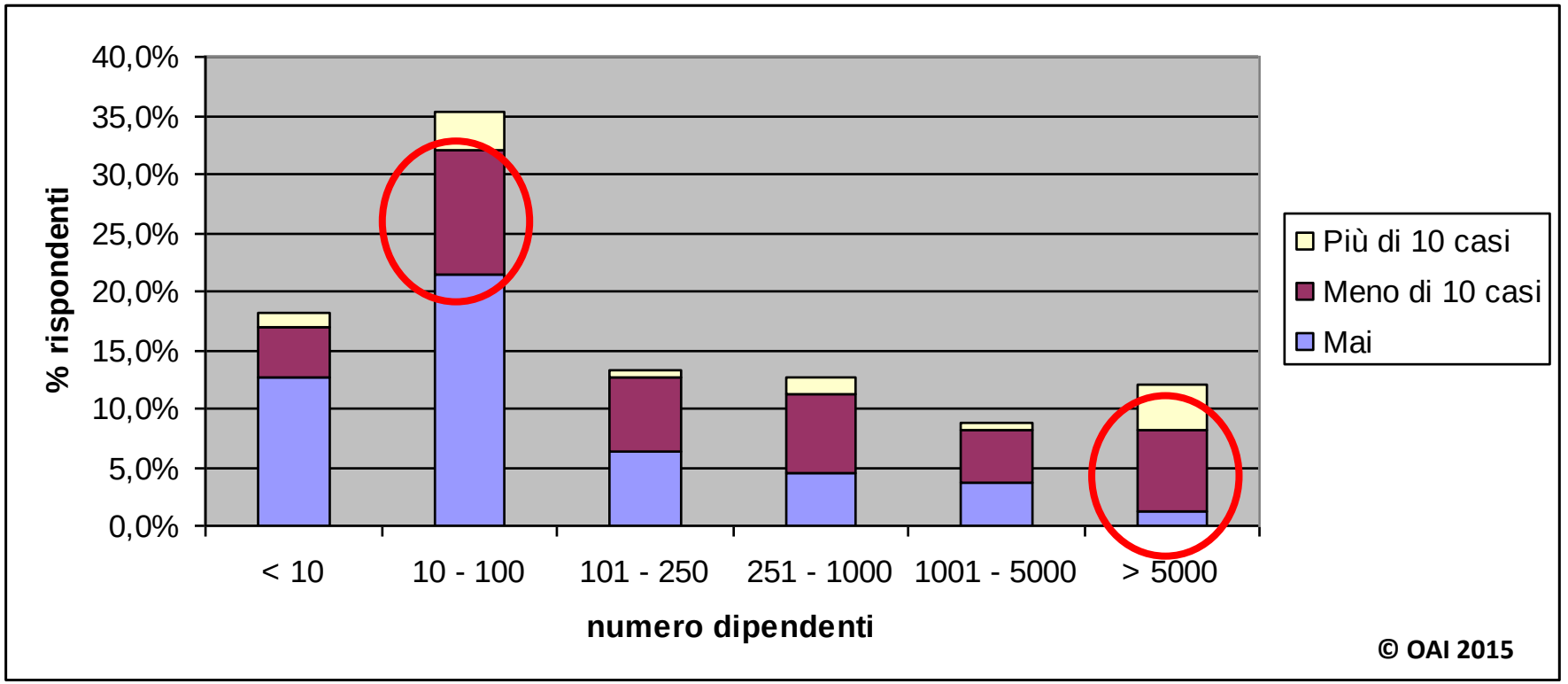
Tempi medi di ripristino dopo un attacco



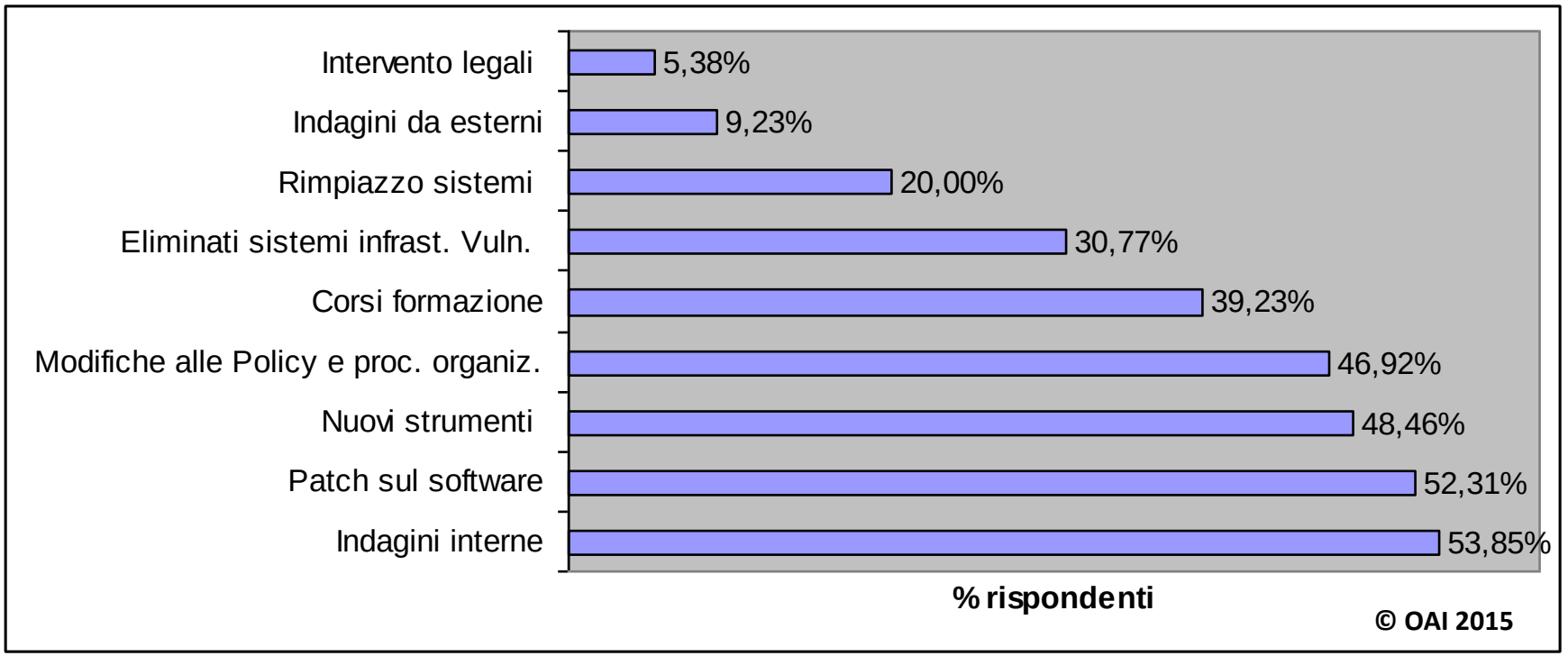
Attacchi 2014 per macro settore



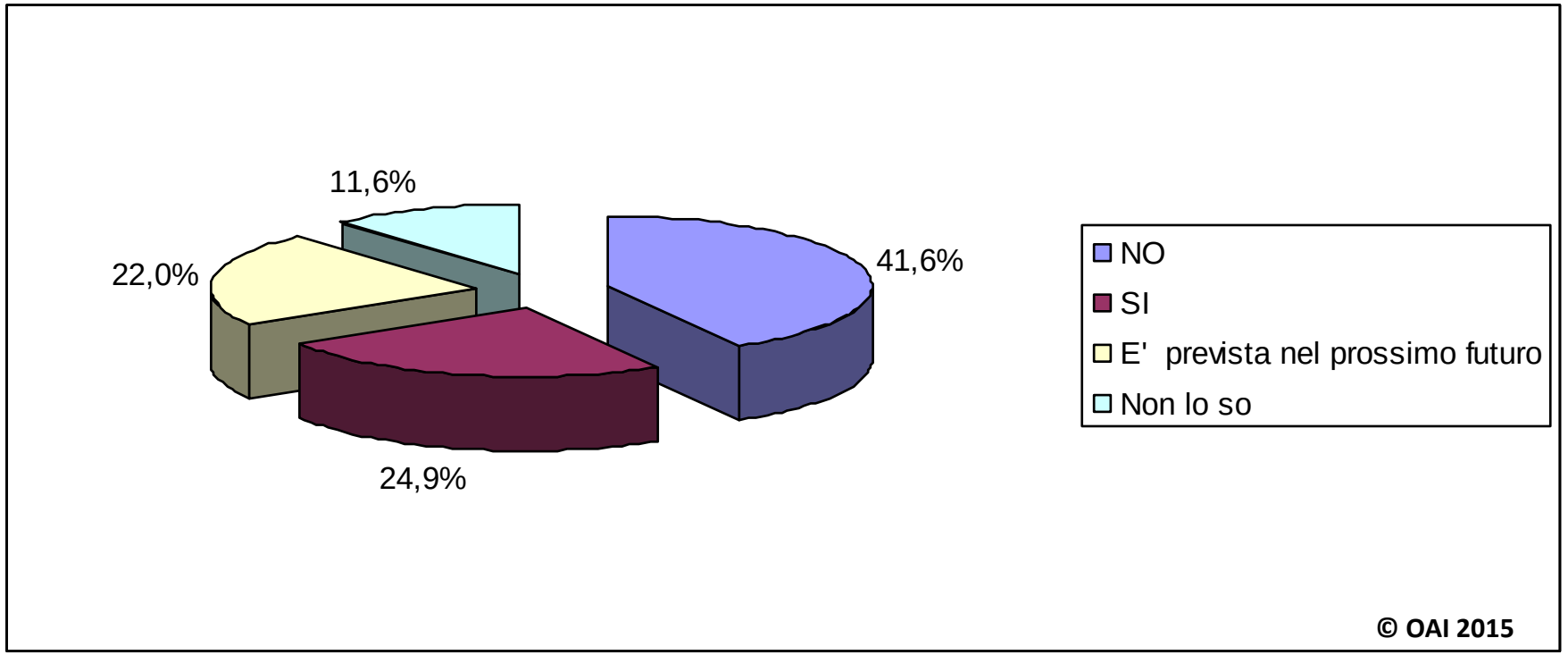
Attacchi 2014 per dimensione dell'azienda/ente



Azioni dopo un attacco



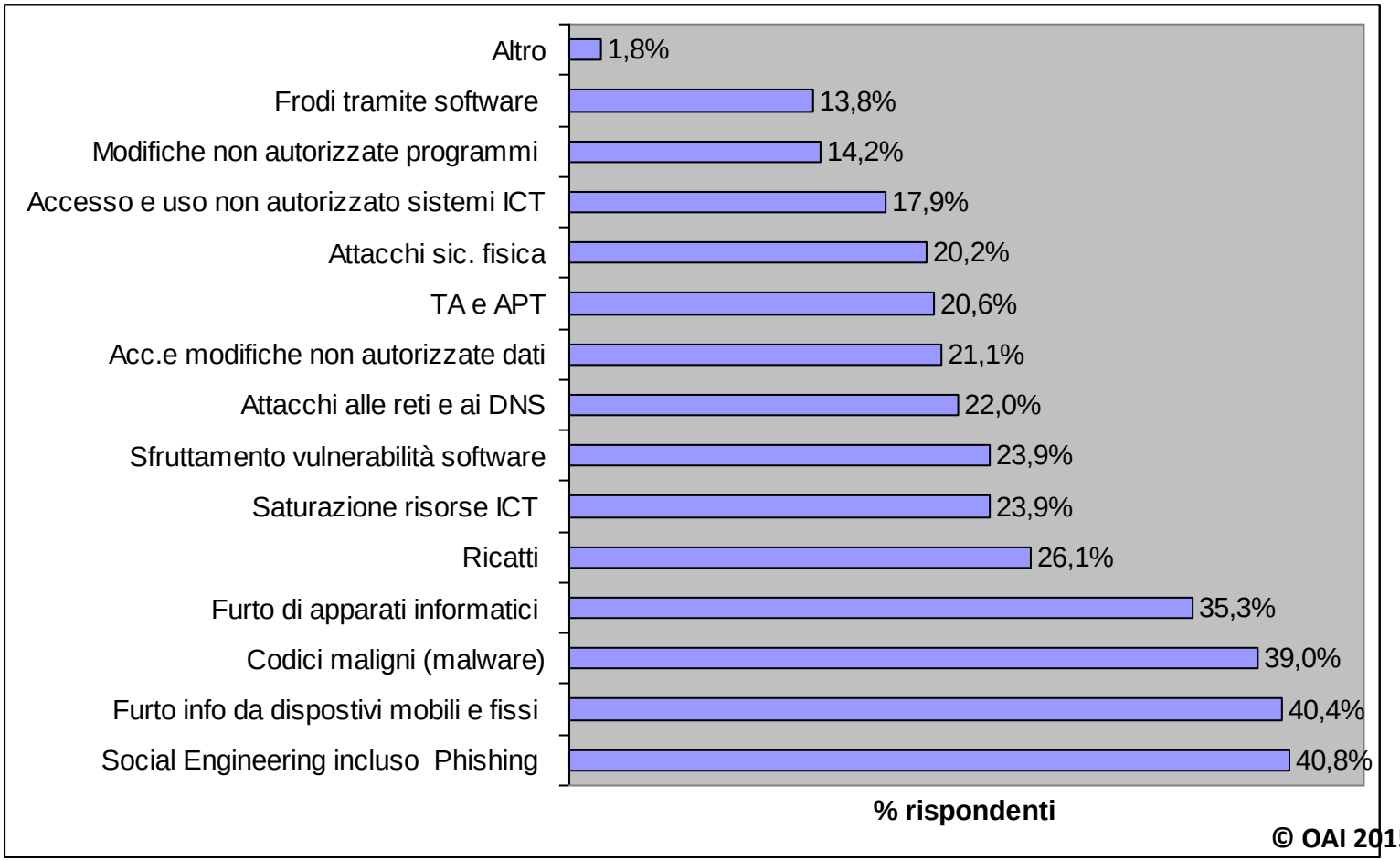
Effettuazione analisi dei rischi ICT



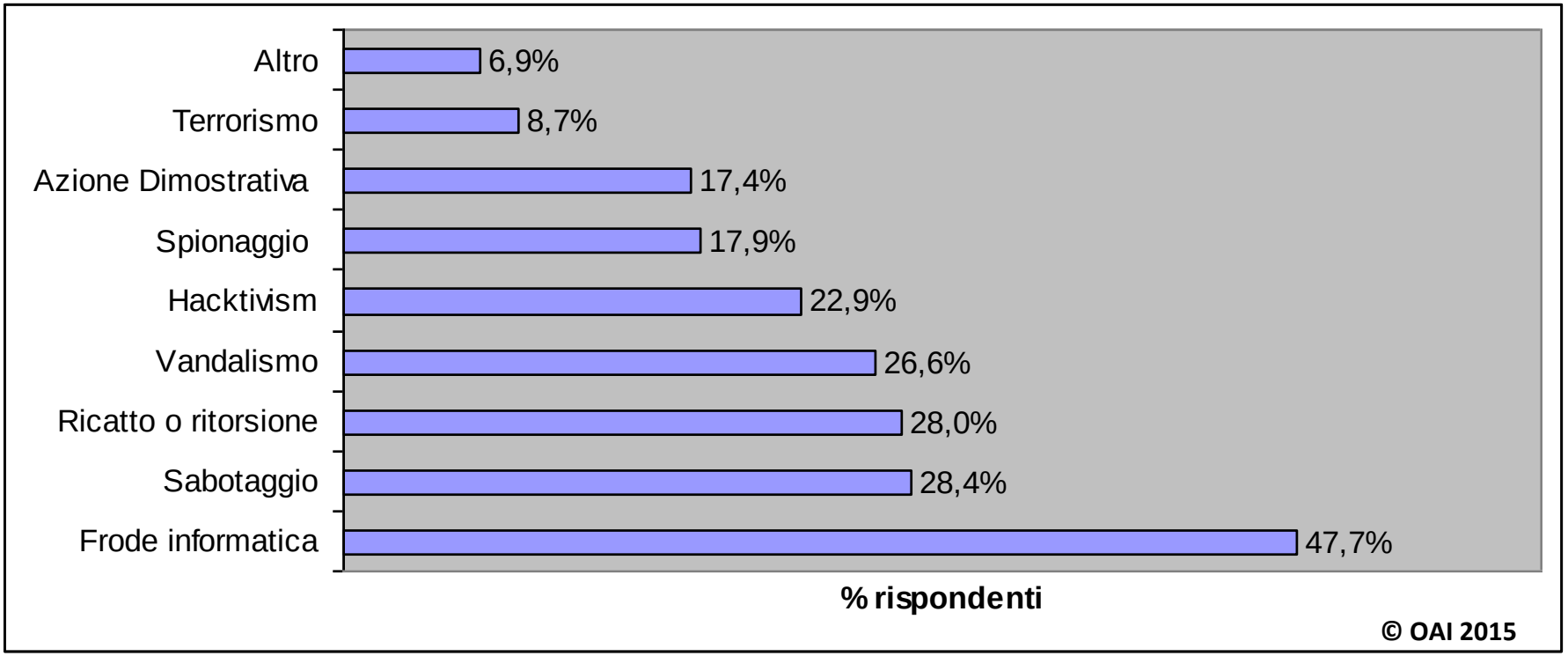
Richiesta conformità standard/best practice e

- ***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%**

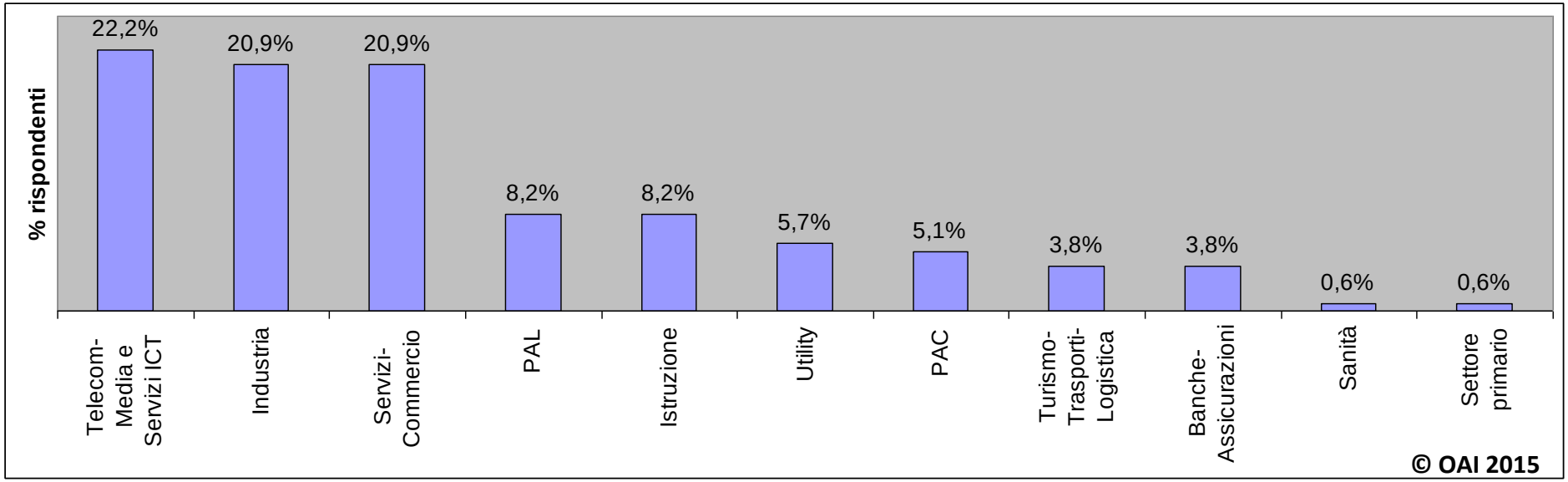
Attacchi maggiormente temuti nel futuro



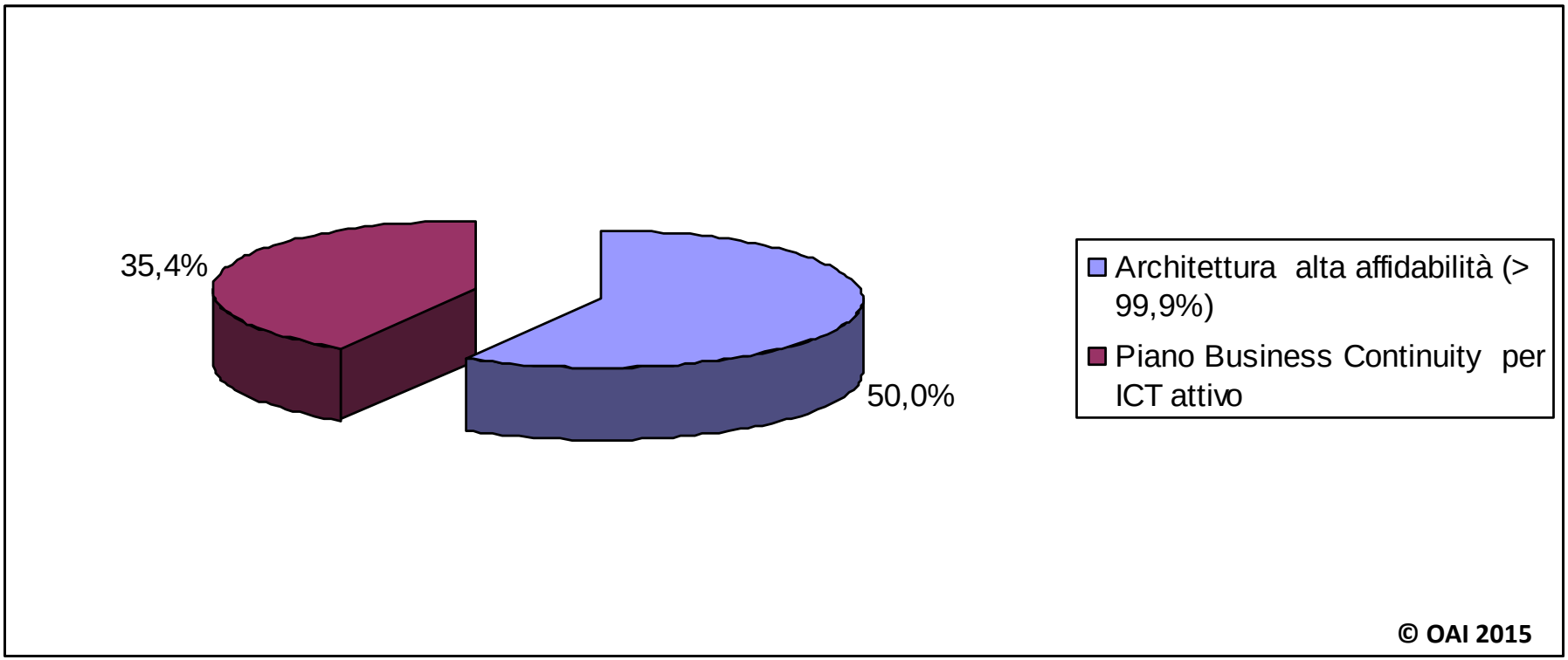
Possibili motivazioni per i futuri attacchi temuti



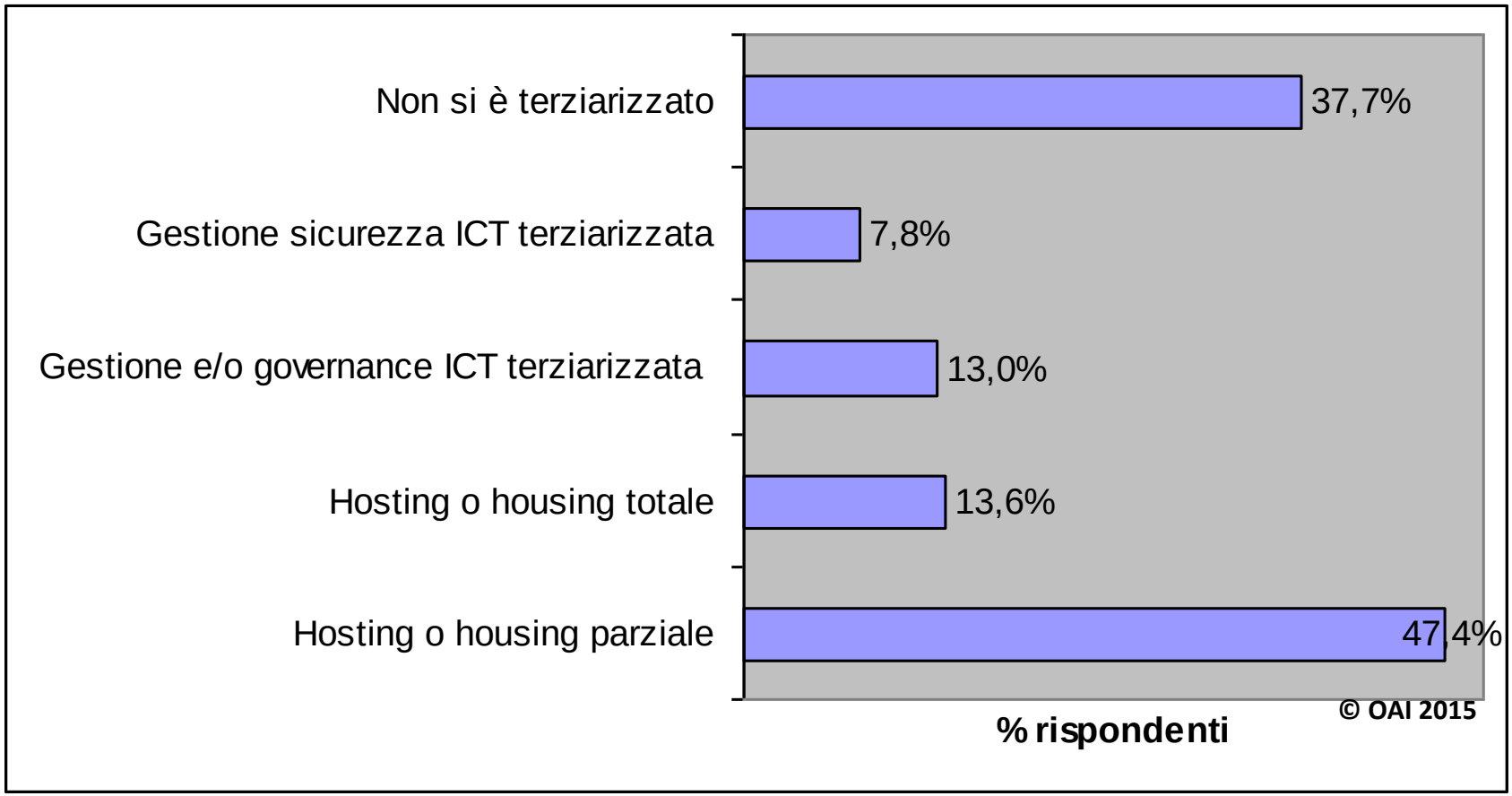
Settore merceologico di appartenenza rispondenti



Alta affidabilità del sistema informatico rispondenti



Uso terziarizzazione rispondenti (risposte multiple)



Come proteggersi ?

La sicurezza globale ICT

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

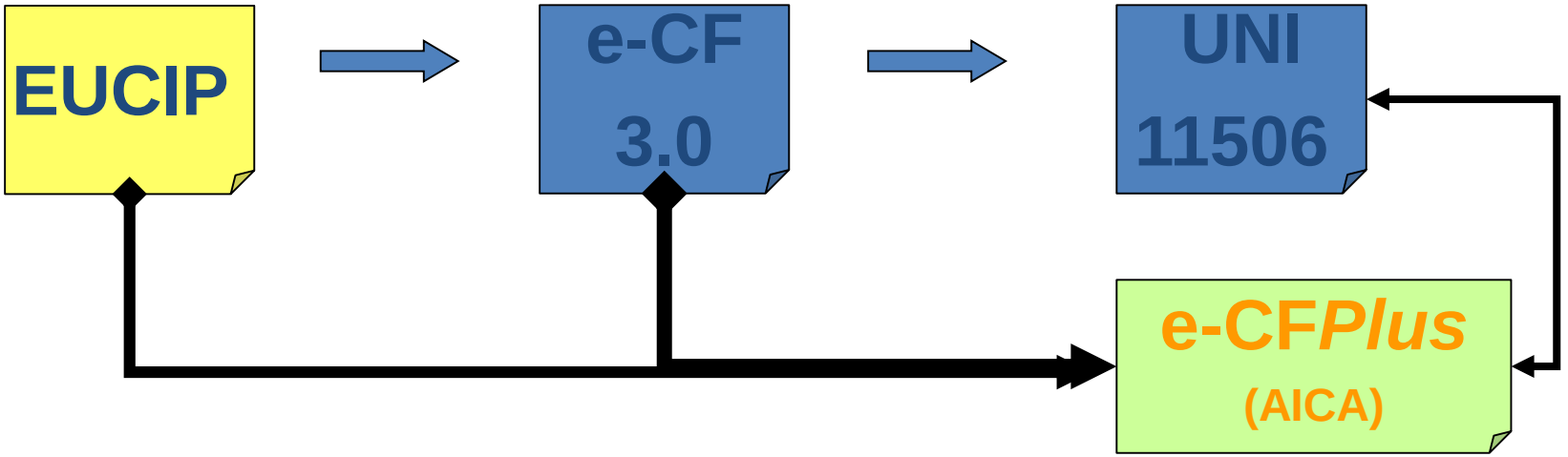
- Non sono burocrazia
- Non sono solo per le grandi strutture
- Sono necessarie anche per la conformità a numerose norme e leggi nazionali ed internazionali
- Includono:
  - Chiara e pubblica definizione di **ruoli** e **competenze**
    - organigramma
    - separazione dei ruoli (**SoD, Separation of 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

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



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
- Prego tutti a gennaio 2016 **a compilare on line il Questionario 2016** !!!

Riferimenti

www.aipsi.org

www.issa.org

www.malaboadvisoring.it