



Marco R.A. Bozzetti

Presidente AIPSI

Ideatore e curatore OAD

CEO Malabo Srl



Osservatorio
Attacchi Digitali
in Italia

Rapporto 2016

Politecnico di Milano, 20 luglio 2016



AIPSI, Associazione Italiana Professionisti Sicurezza Informatica

- <http://www.aipsi.org/>
- **Capitolo italiano di ISSA**, Information Systems Security Association, (www.issa.org)
 - >>10.000 Soci, la più grande associazione non-profit di professionisti della Sicurezza ICT
- **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**
 - **Aiutare i propri Soci nella crescita professionale e quindi del loro business**
 - **offrire ai propri Soci qualificati servizi per tale crescita**
 - **diffondere la cultura e la sensibilizzazione per la sicurezza informatica agli utenti digitali,**
- **Sedi territoriali** : Milano, Ancona-Macerata, Roma, Lecce
- **Collaborazione** con varie associazioni ICT ed Enti per eventi ed iniziative congiunte: AICA, Anorc, i vari ClubTI sul territorio, CSA Italy, FidaInform, Inforav, Polizia Postale, Smau, ecc.



OAD, Osservatorio Attacchi Digitali in Italia (ex OAI)

- Che cosa è

- 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



Osservatorio
Attacchi Digitali
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
- Gruppo OAI su Linked

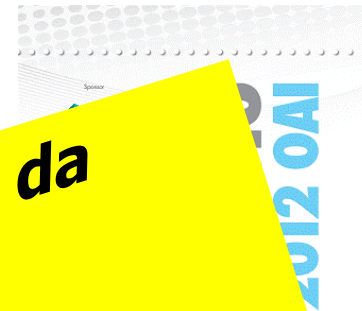


- Come

- 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



Le precedenti edizioni OAI



I precedenti Rapporti scaricabili da

<http://www.aipsi.org/>

<http://www.malboadvisoring.it/>



Rapporto 2016 OAD



Per poter avere il Rapporto 2016 lasciare il biglietto da visita con email: verrà inviato il codice coupon per scaricarlo

Sponsorizzazioni e patrocini OAD 2016

Sponsor Gold



Sponsor Silver



con la collaborazione di



Patrocinatori



Indice del Rapporto 2016

1. Executive Summary in Italiano e in Inglese
 2. Introduzione
 3. Le tipologie di attacco considerate
 4. Gli attacchi informatici rilevati
 - 4.1 Gli impatti dagli attacchi subiti
 - 4.2 Gli attacchi alle infrastrutture critiche italiane: i dati dalla Polizia Postale e delle Comunicazioni e dal C.N.A.I.P.I.C.
 - 4.3 Financial Cybercrime
 - 4.5 Nuovi e vecchi attacchi
 - 4.6 La situazione a livello europeo secondo ENISA
 5. L'individuazione e la gestione degli attacchi
 6. Strumenti e misure di sicurezza ICT adottate
 - 6.1 Sicurezza fisica
 - 6.2 Sicurezza logica
 - 6.3 Gli strumenti per la gestione della sicurezza digitale
 - 6.4 Le misure organizzative
 7. Gli attacchi più temuti nel futuro e le probabili motivazioni
- Allegato A - Aspetti metodologici dell'indagine OAD
- Allegato B - Il campione emerso dall'indagine
- Allegato C - Profili Sponsor
- Allegato D – Riferimenti e fonti
- Allegato E - Glossario dei principali termini ed acronimi sugli attacchi informatici
- Allegato F - Profilo dell'Autore
- Allegato G - Malabo Srl
- Allegato H - Nextvalue Srl
- Allegato I - Note

• **128 pagine A4**

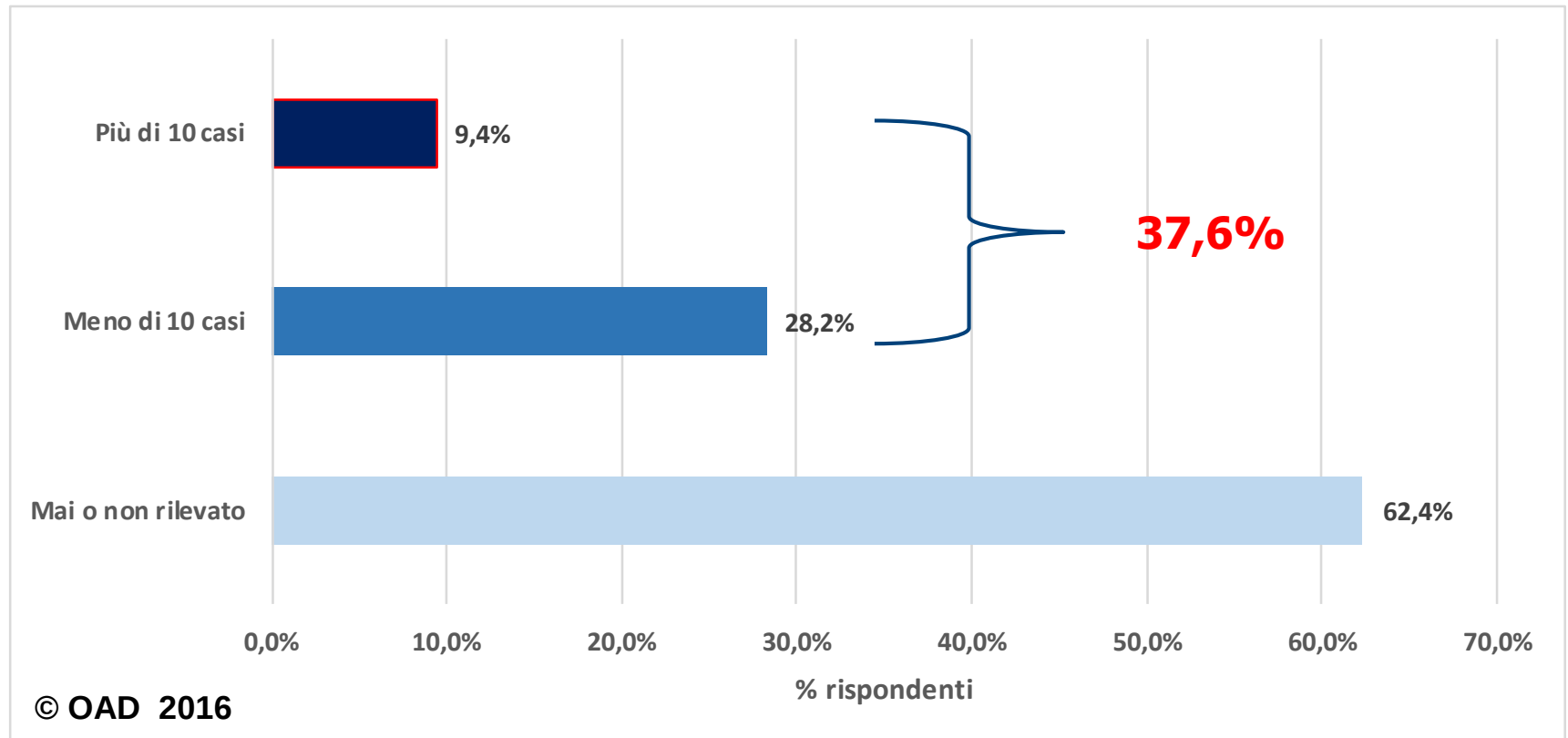
• **5 Tabelle**

• **67 Grafici**

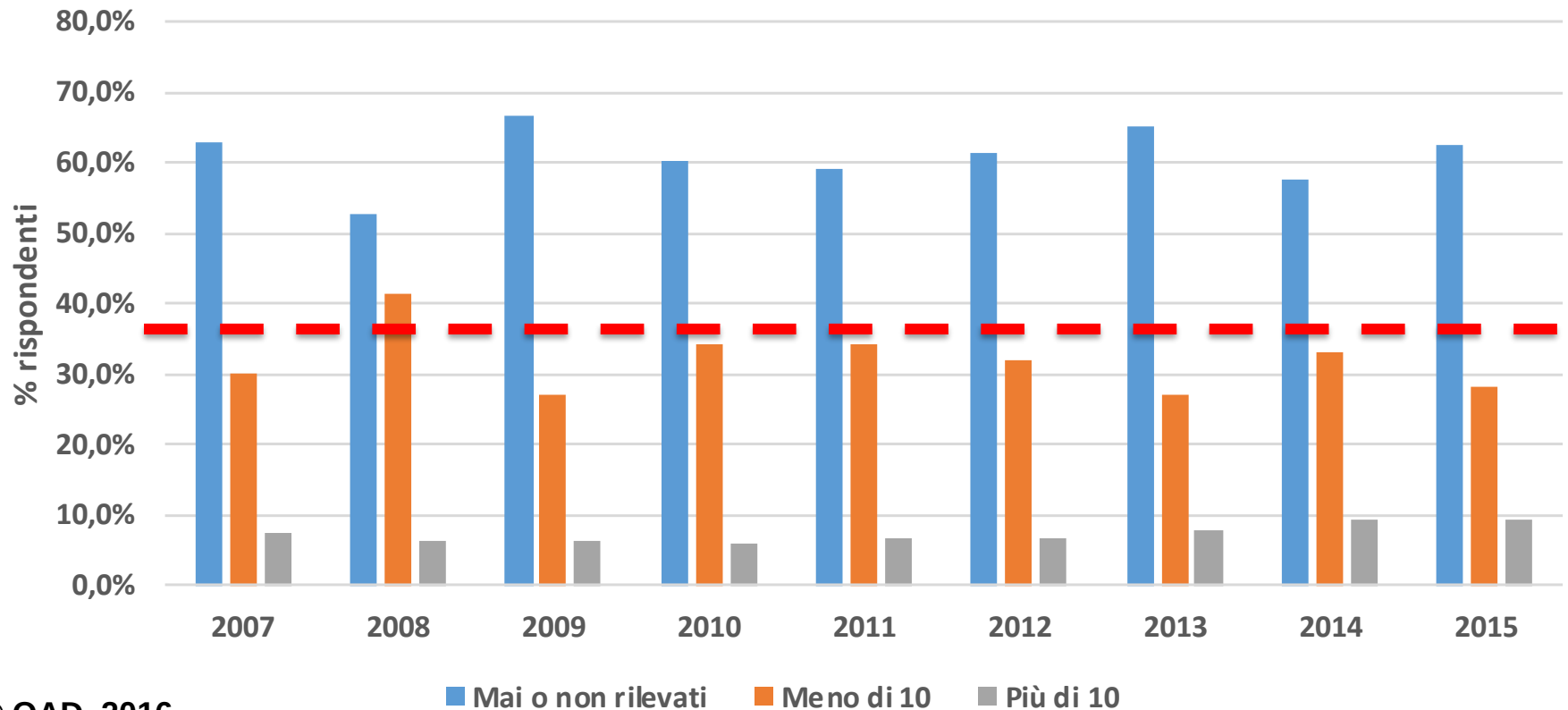
Le risposte al Questionario 2016 OAD

- Questionario online via web con 65 domande e risposte, multiple o singola, da selezionare con un click tra quelle predefinite
- Risposte completamente anonime
- Coinvolti potenziali rispondenti dalle mailing list di AIPSI, di Malabo, di NextValue, dei Patrocinatori
- **288 rispondenti in totale**

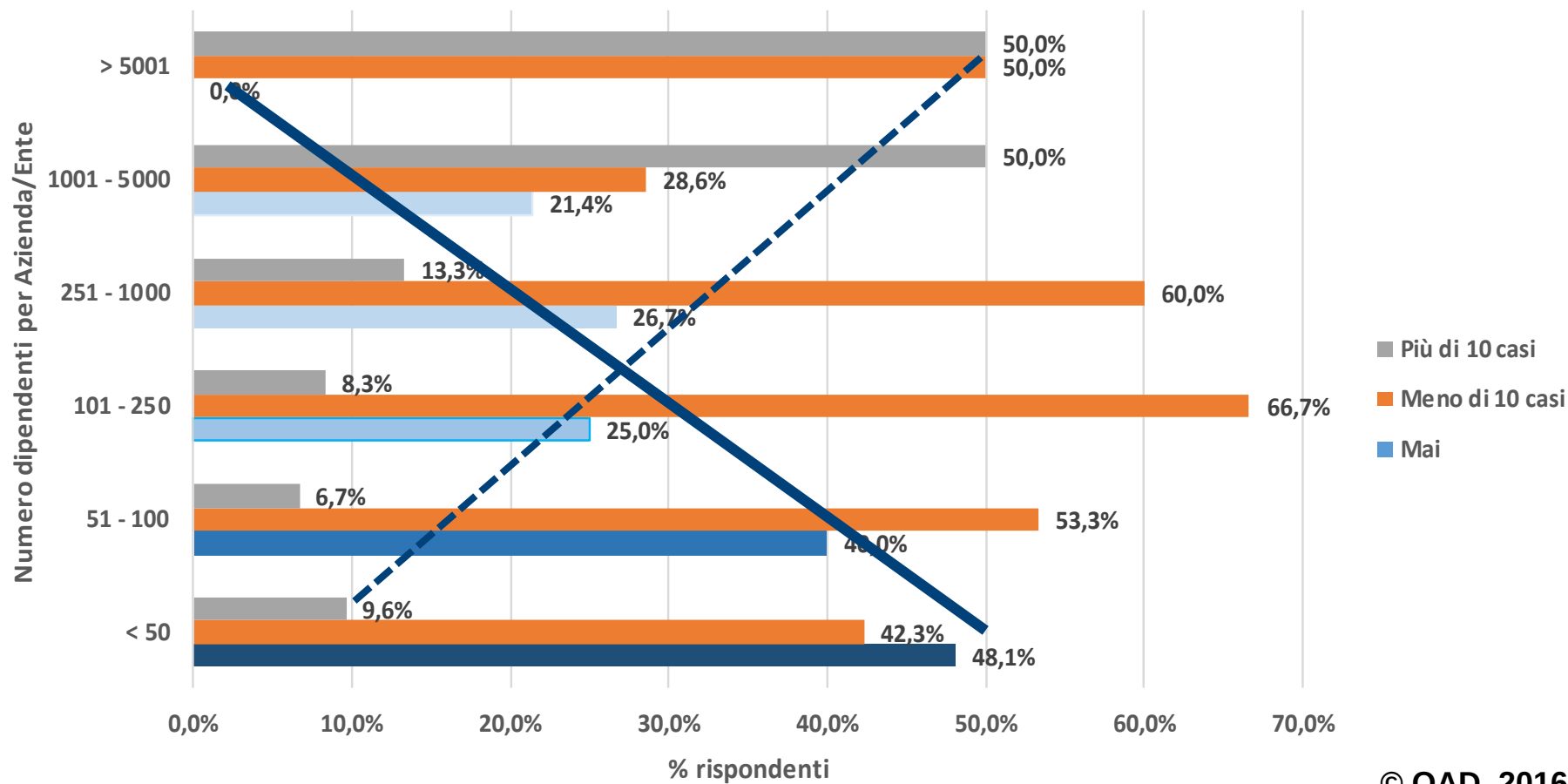
Attacchi rilevati nel 2015



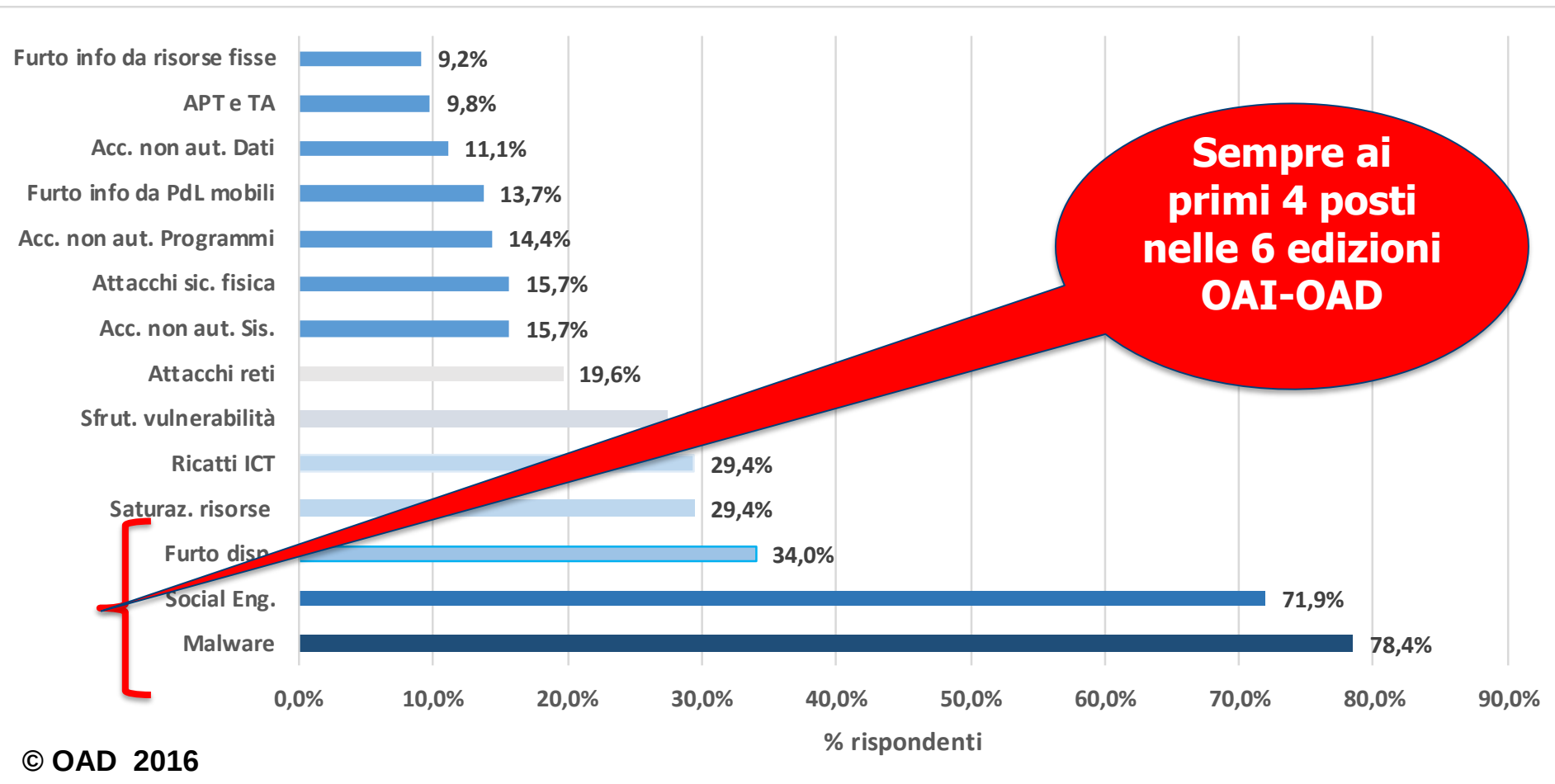
Confronto percentuale degli attacchi rilevati nelle varie edizioni di OAI-OAD (indicatore di trend NON STATISTICO)



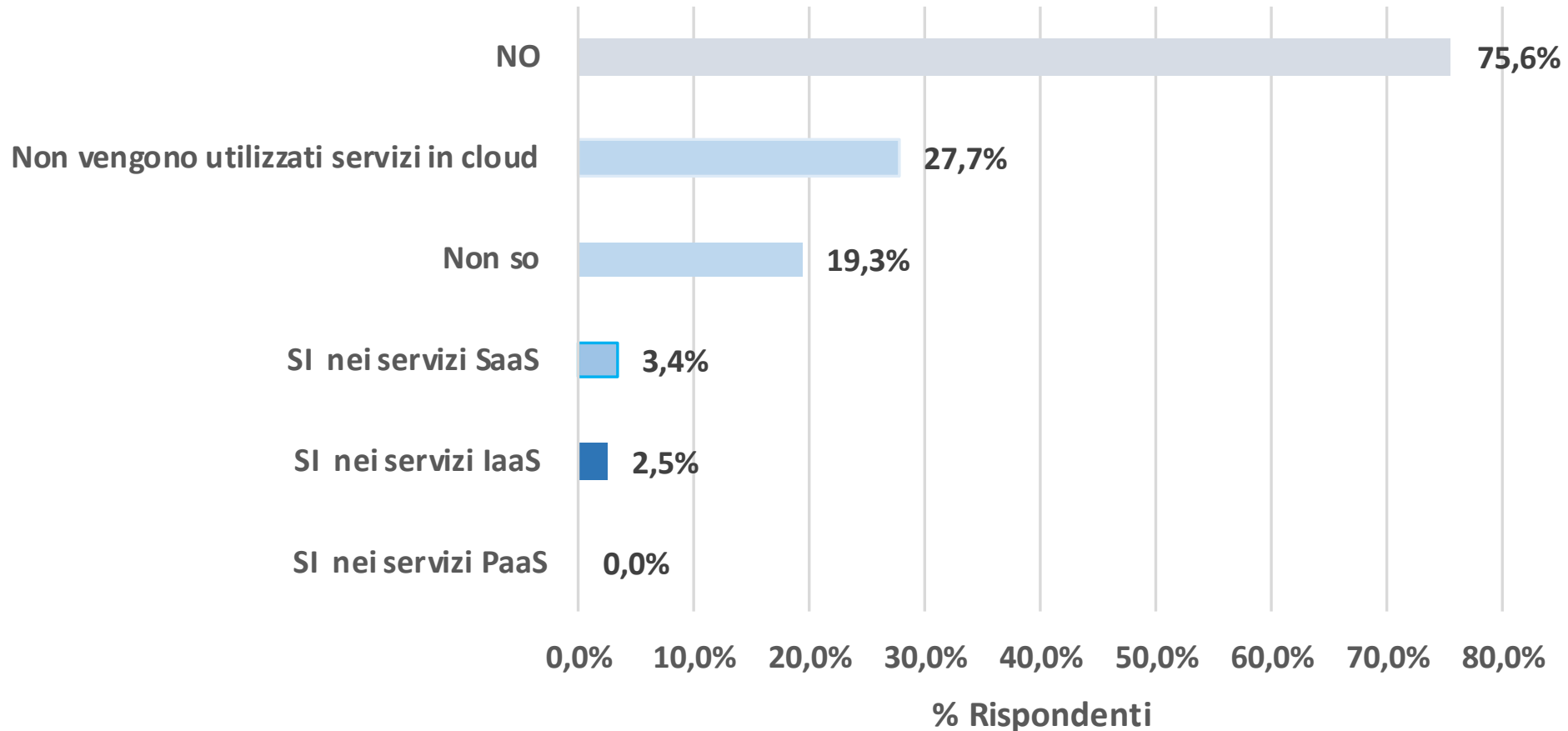
Percentuale numero di attacchi ripartiti per dimensione di azienda/ente



Ripartizione percentuale per tipologia di attacco (risposte multiple)

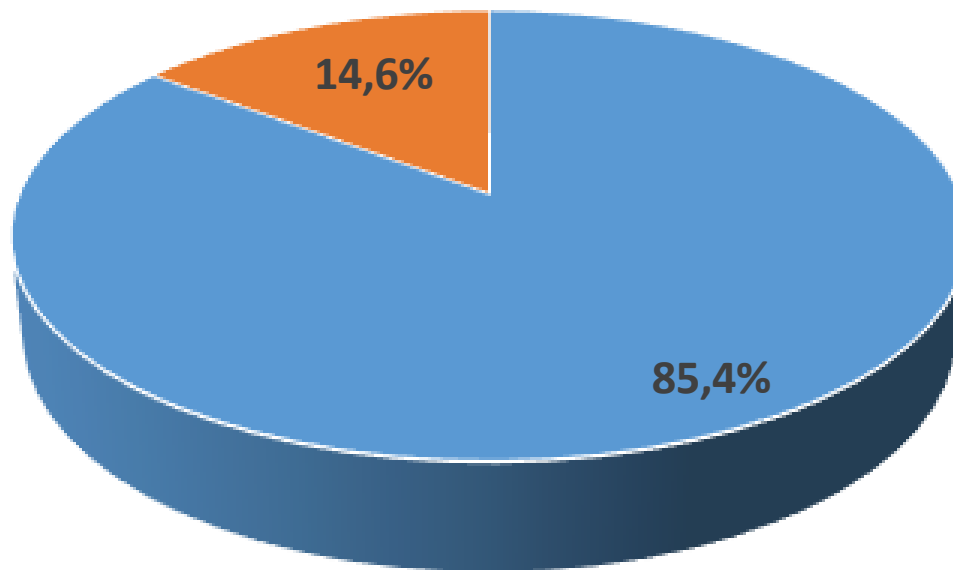


Attacchi nei servizi in cloud (risposte multiple)



Impatto degli attacchi subiti

© OAD 2016



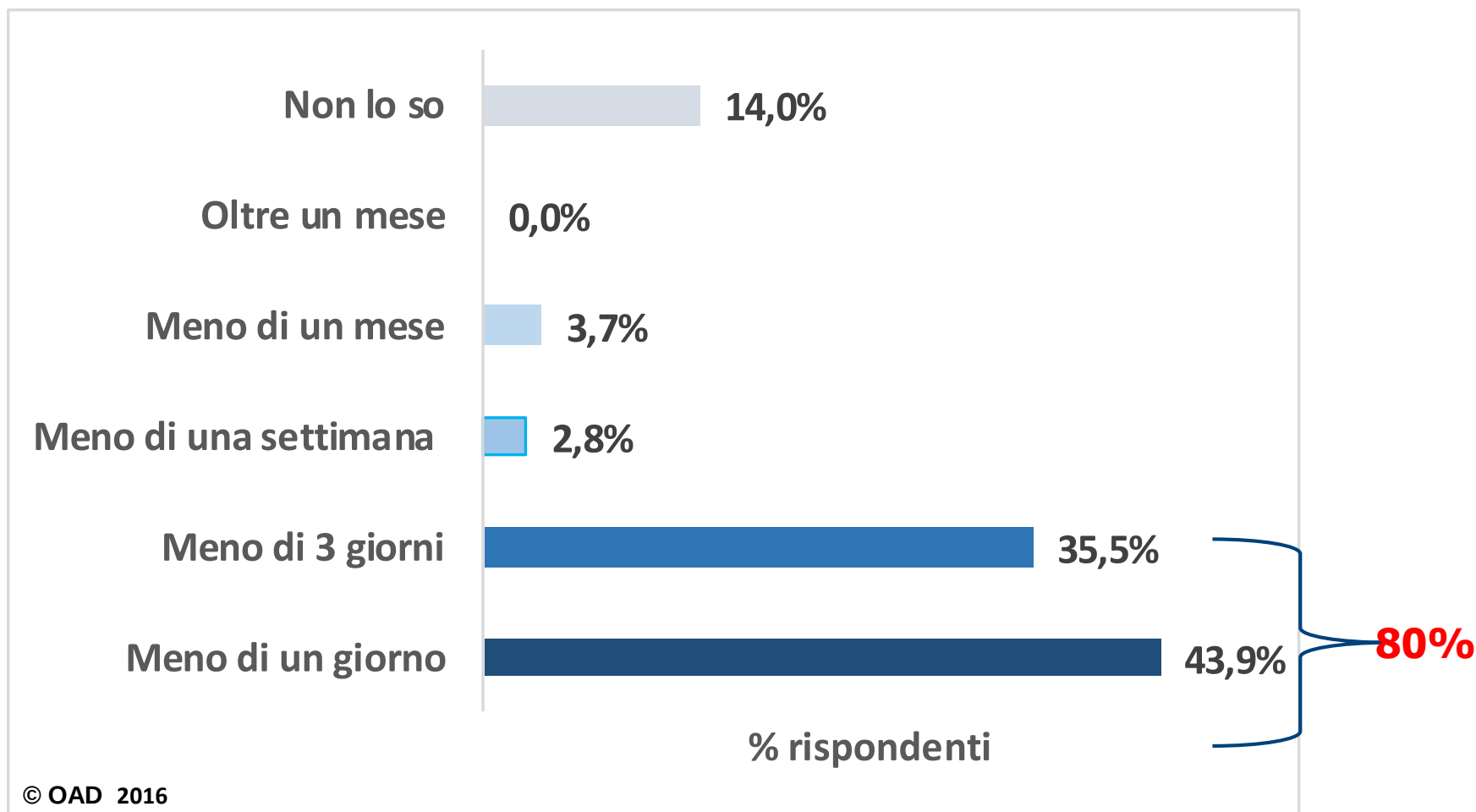
■ Impatto poco significativo ■ Impatto molto significativo

Valori medi e massimi dei costi economici degli attacchi subiti nel 2015 (Fonte OAD 2016)

Valore medio costo del singolo attacco più grave	3.605,3
Valore più alto del costo del singolo attacco più grave	€ 70.000,00
Valore medio del costo complessivo di tutti gli attacchi subiti nel 2015	€ 6.013,30
Valore più alto del costo complessivo di tutti gli attacchi subiti nel 2015	€ 120.000,00

© OAD 2016

Tempo massimo occorso per il ripristino dei sistemi ICT



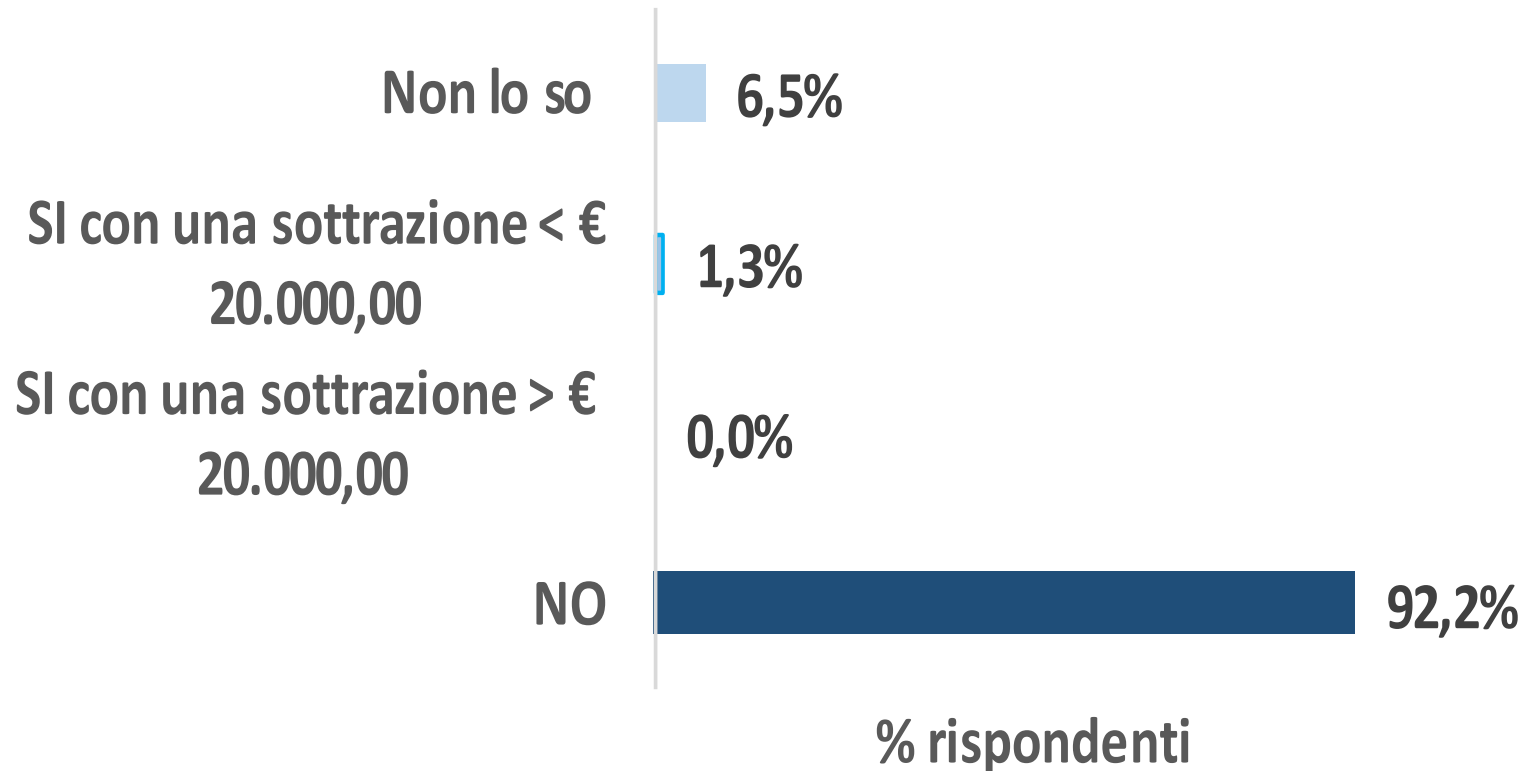
Statistiche generali attività C.N.A.I.P.I.C. nel 2015

(Fonte: Polizia Postale e delle Comunicazioni)

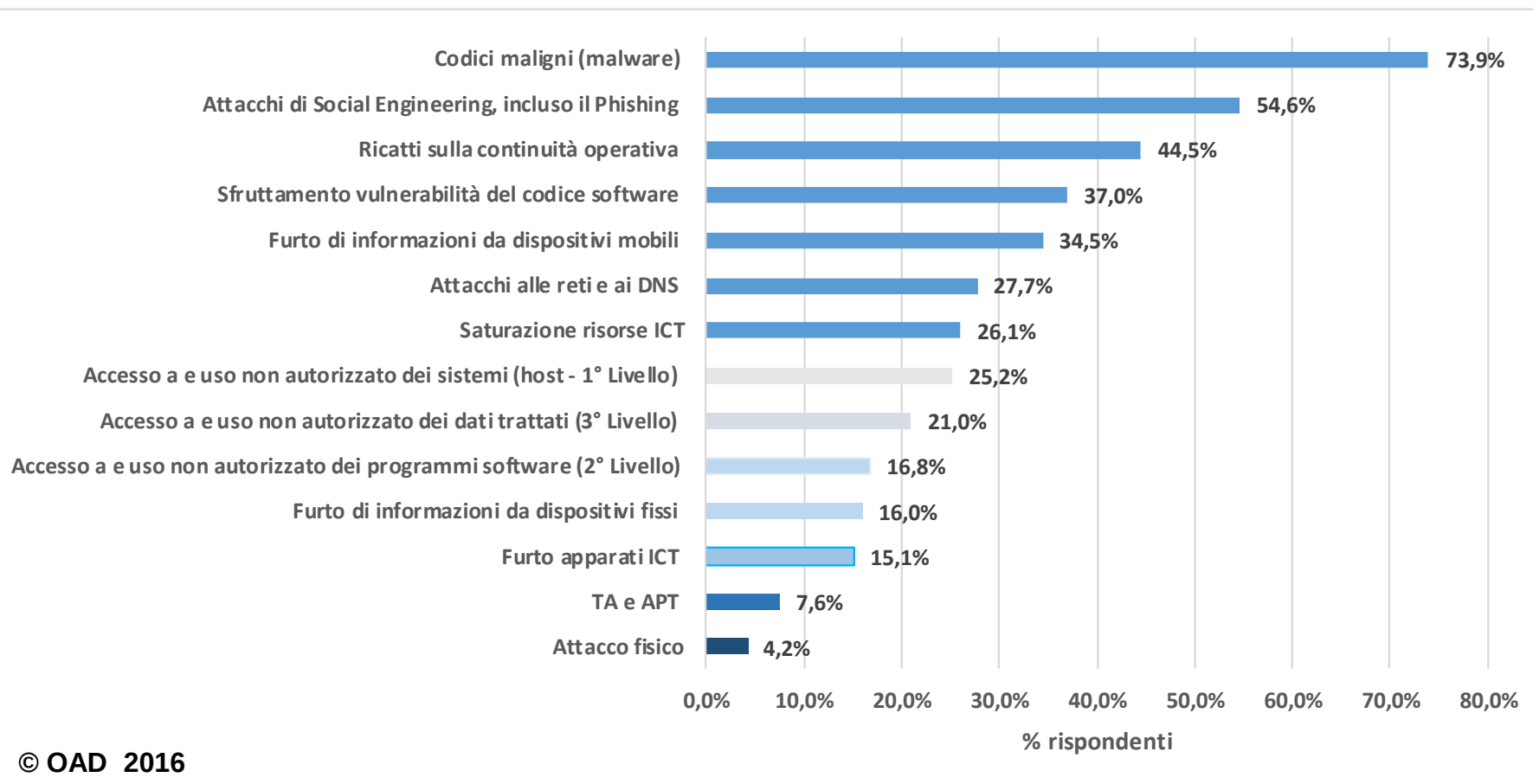
Attacchi rilevati	633
Alert diramati	987
Monitoraggi	13500
Indagini avviate	55
Persone denunciate	44
Persone arrestate	2
Richieste di cooperazione High Tech Crime Network	95

© OAD 2016

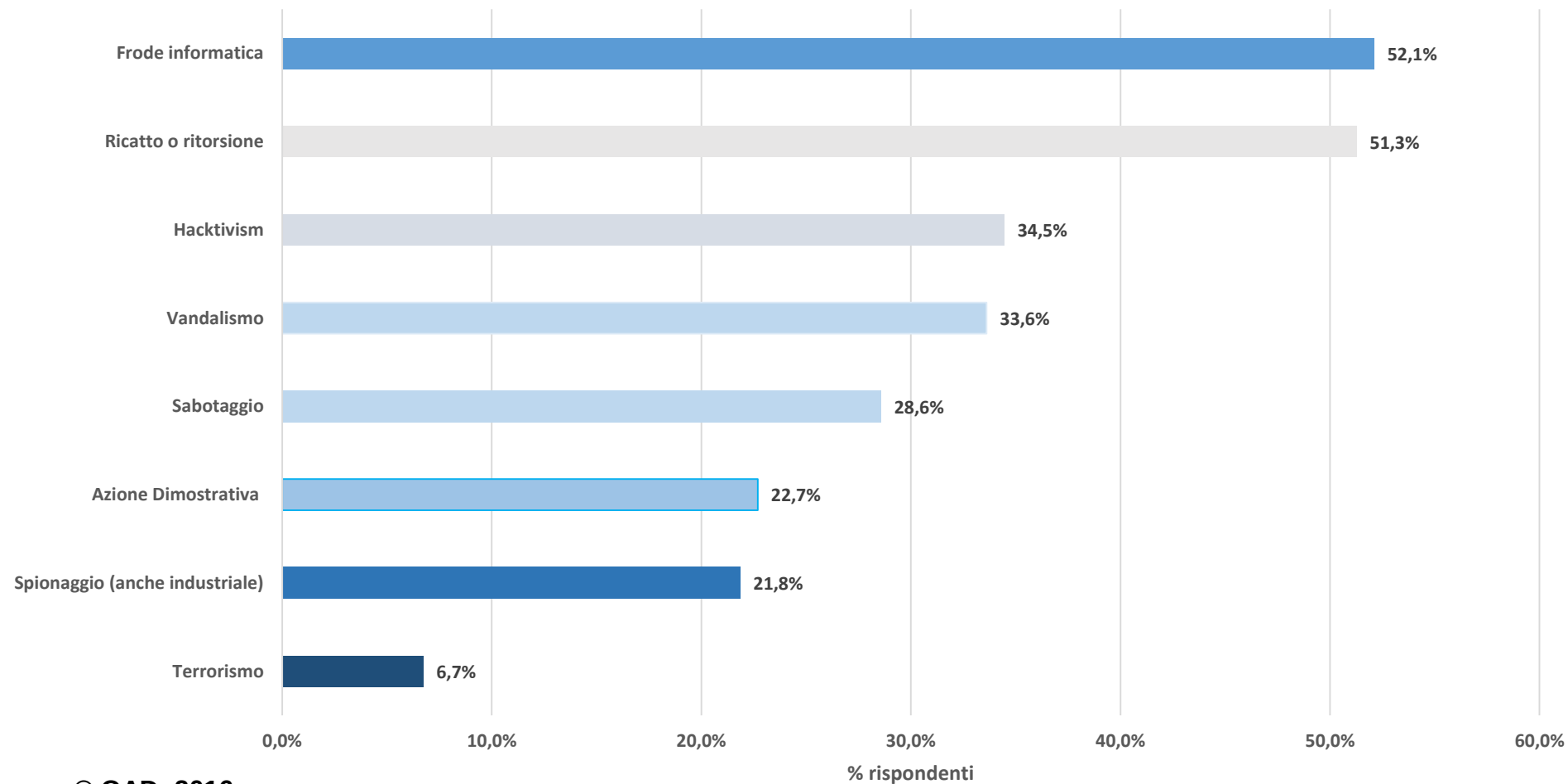
Sottrazioni di denaro sui conti bancari nel 2015 causati da furto di identità digitale



Quali gli attacchi più temuti nel prossimo futuro? (risposte multiple)



Quali le motivazioni degli attacchi? (risposte multiple)



Sintesi attività Polizia Postale di contrasto al cyber-terrorismo ed ai reati di odio

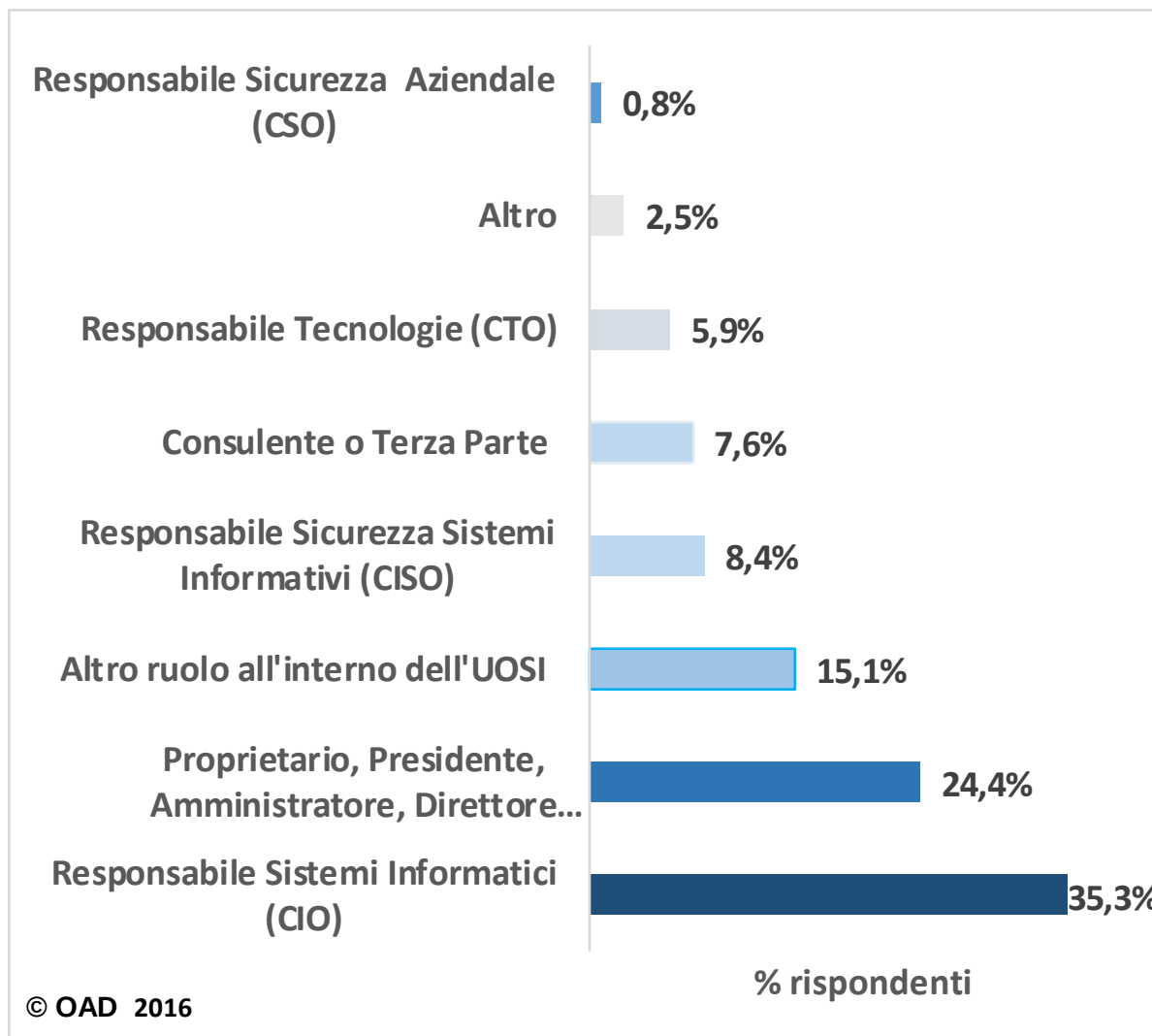
(Fonte: Polizia Postale e delle Comunicazioni)

Spazi web monitorati	
Spazi web (siti, forum, blog, media di informazione, profili twitter e facebook) verificati	11833
Spazi web monitorati	580
Accertamenti in cooperazione con altri Enti	268
Contenuti web oscurati direttamente dal Gestore del Servizio	6612
Contenuti web oscurati su segnalazione della Polizia Postale	23
Segnalazioni ricevute dai cittadini tramite Commissariato di PS On line	
Spazi web segnalati	179
Spazi web riconducibili al terrorismo	71
Atti discriminatori nei confronti delle minoranze	
Segnalazioni	541
Link	192
Denunciati	12
Attività anti terrorismo	
Denunciati	3
Arrestati	0

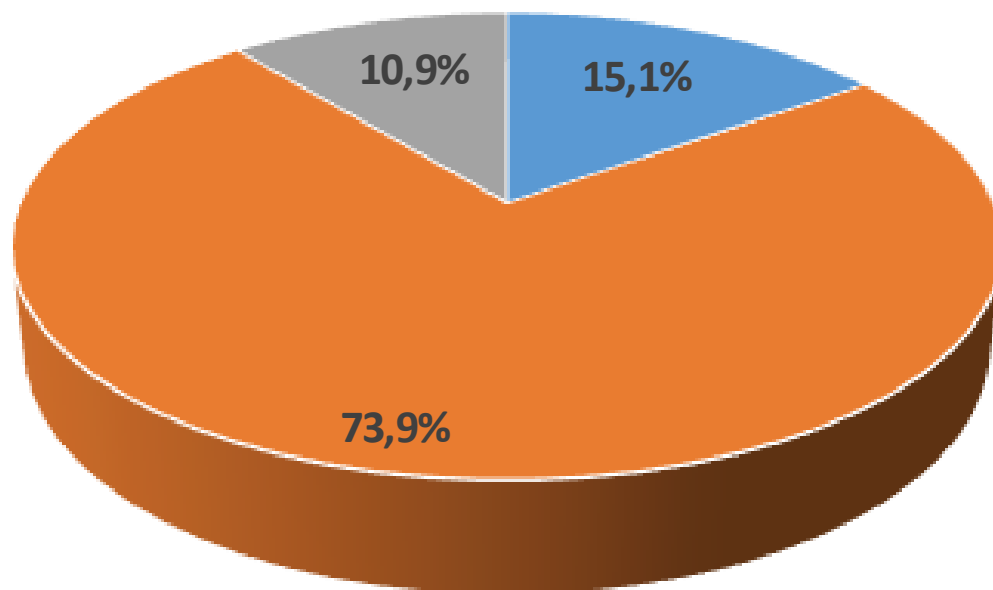
© OAD 2016

Il campione emerso

Ruolo dei rispondenti



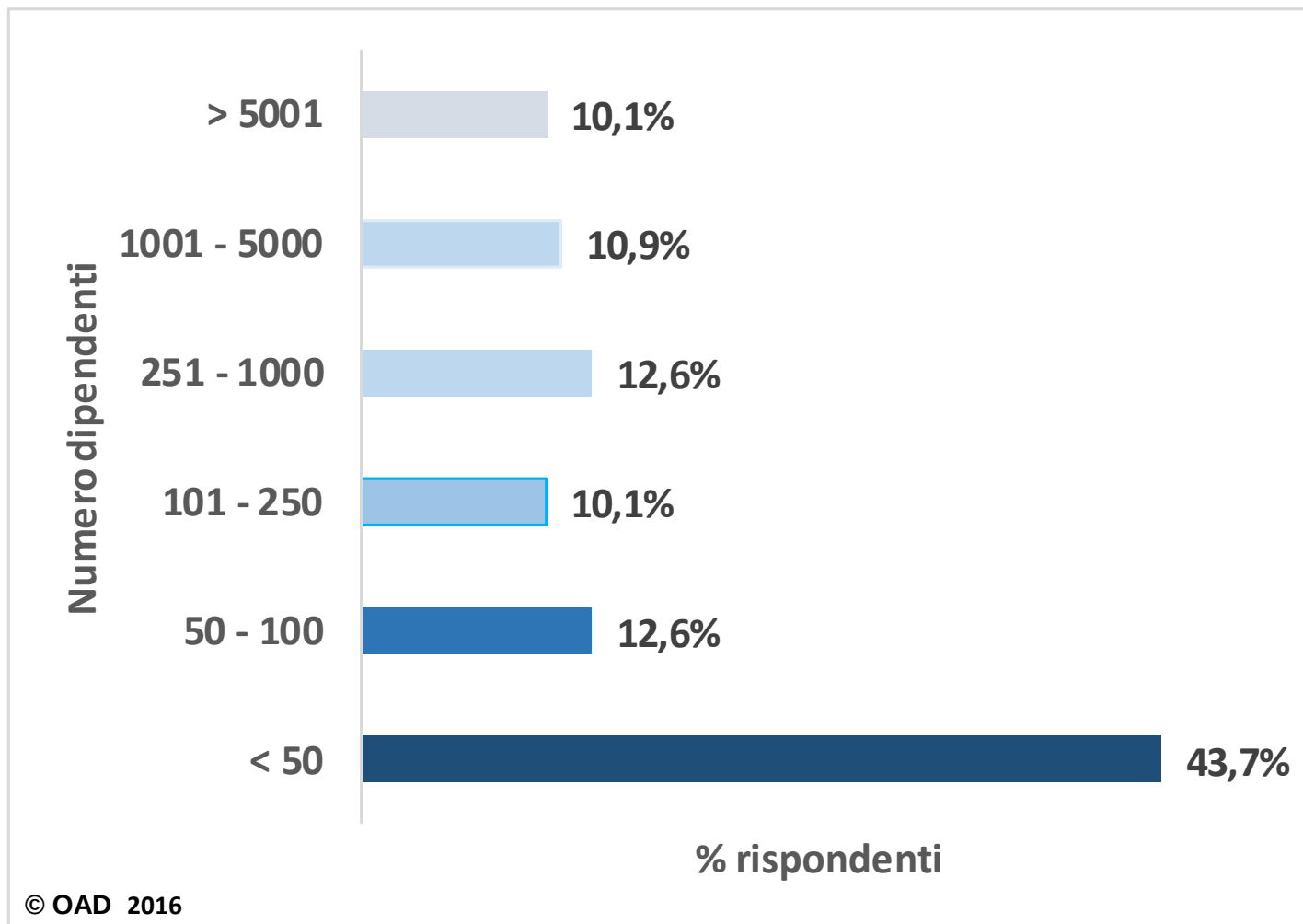
Macro-settori merceologici delle aziende/enti dei rispondenti



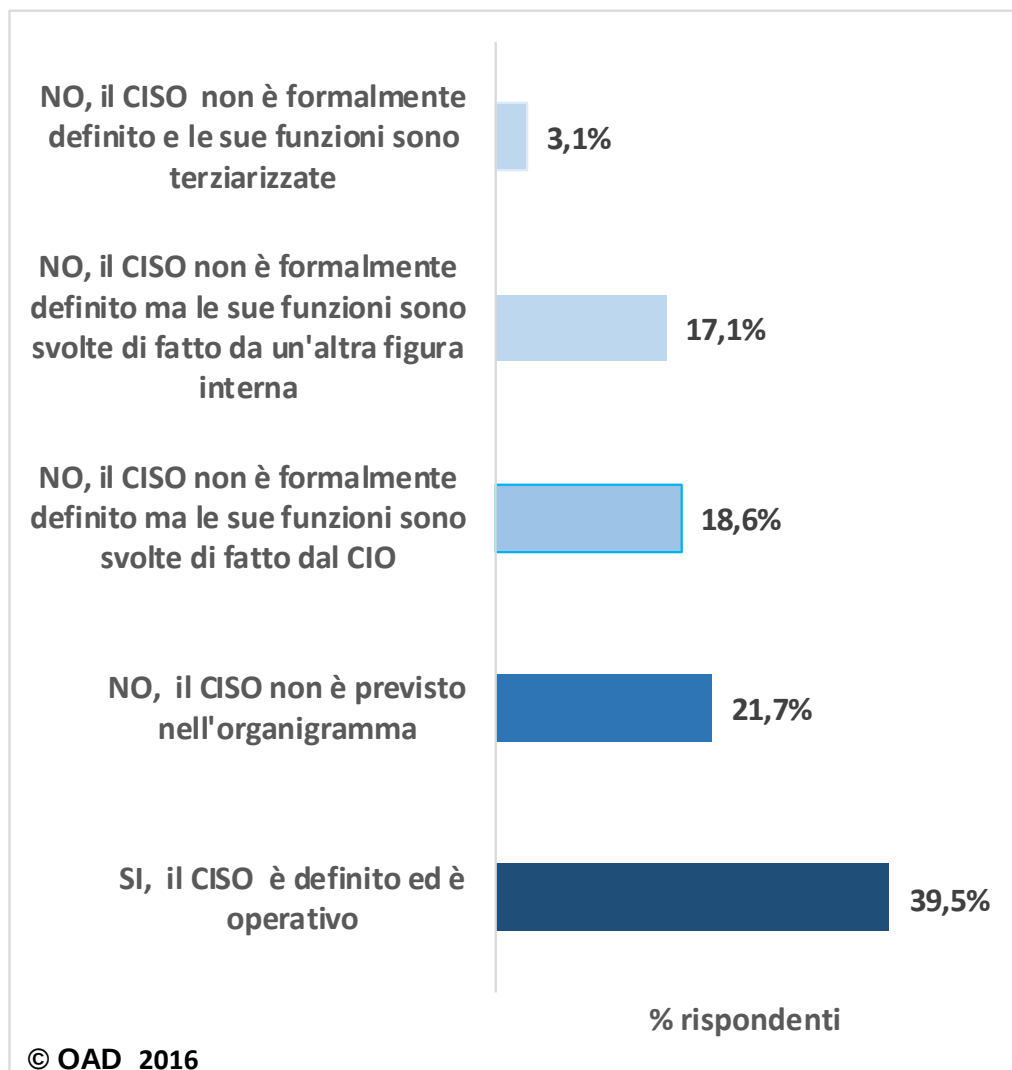
■ Secondario ■ Terziario ■ PA

© OAD 2016

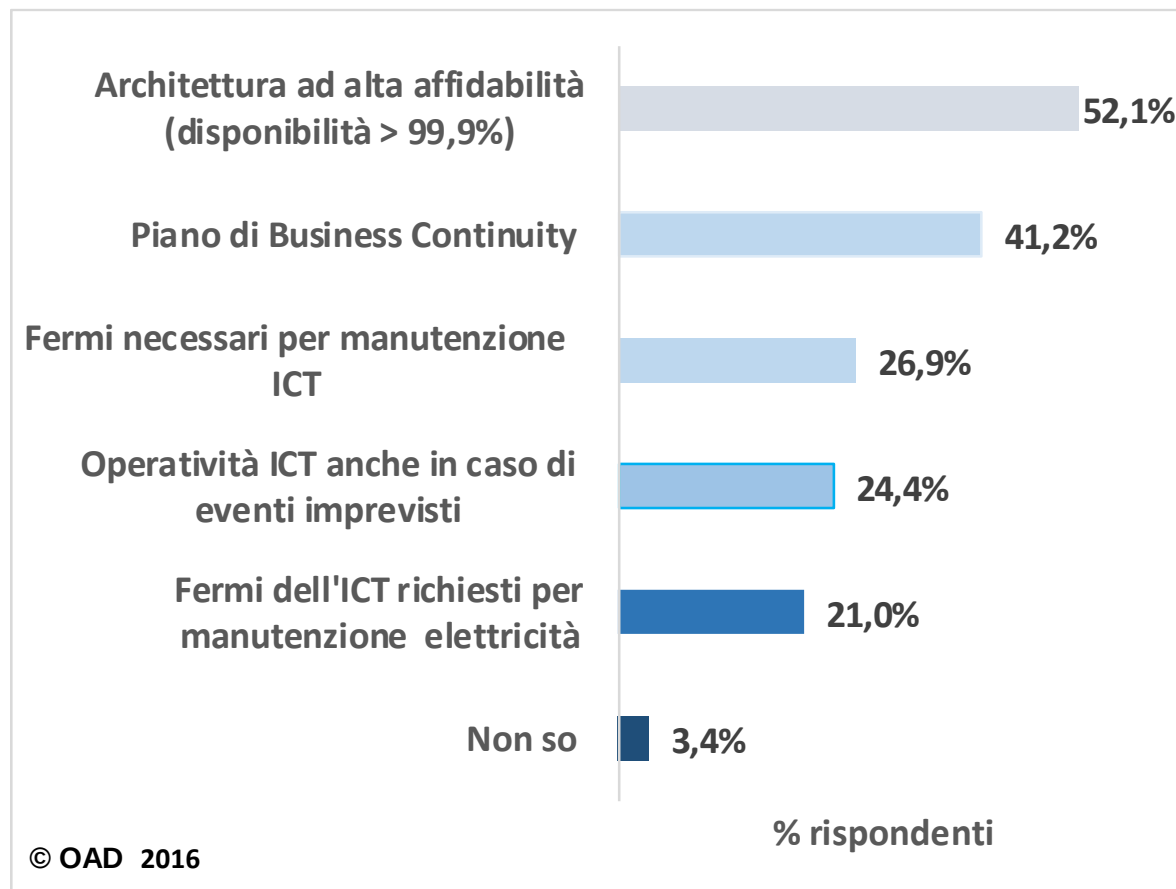
Dimensioni aziende/enti dei rispondenti per numero di dipendenti



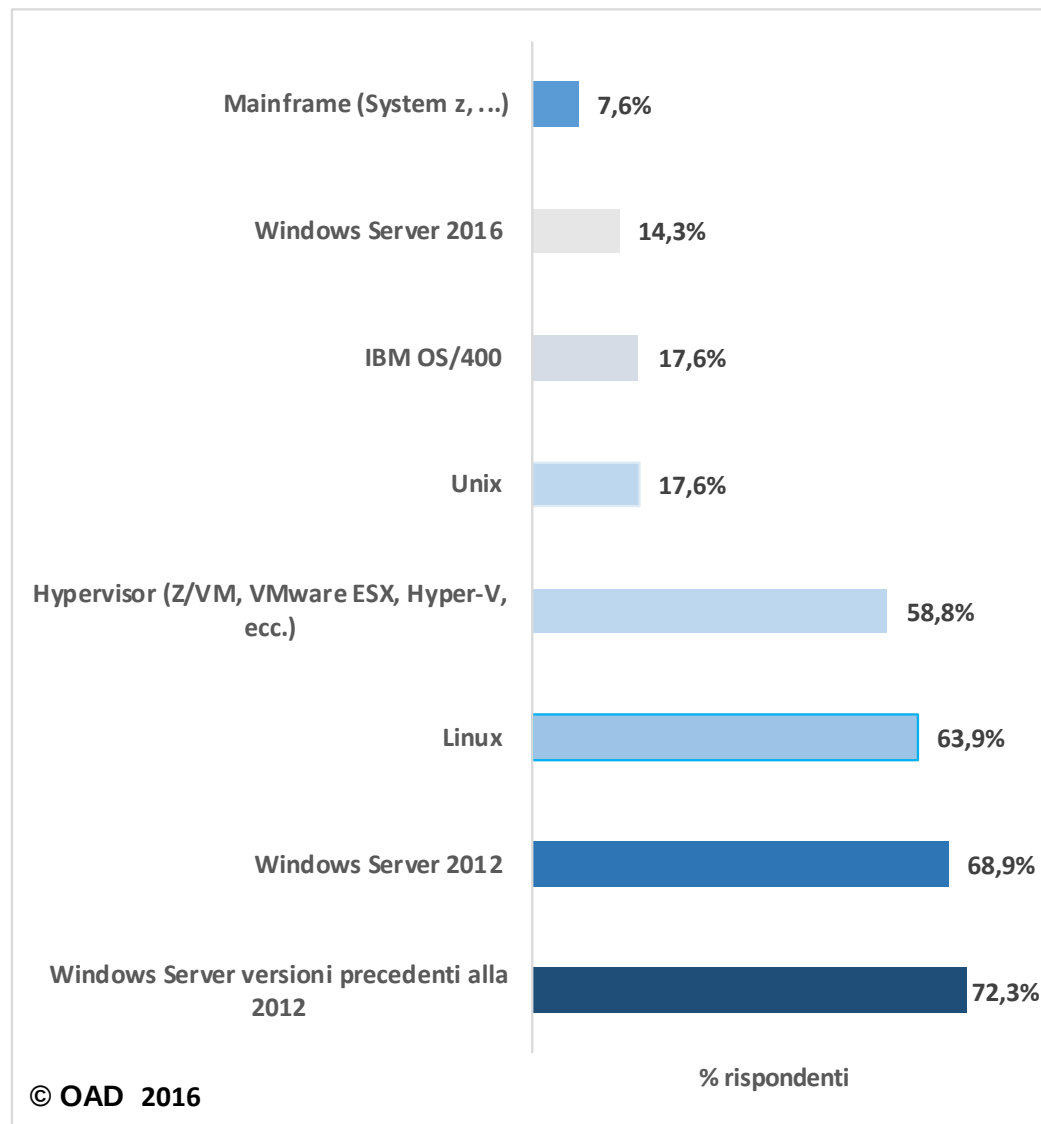
Esistenza del ruolo di responsabile della sicurezza digitale (CISO)



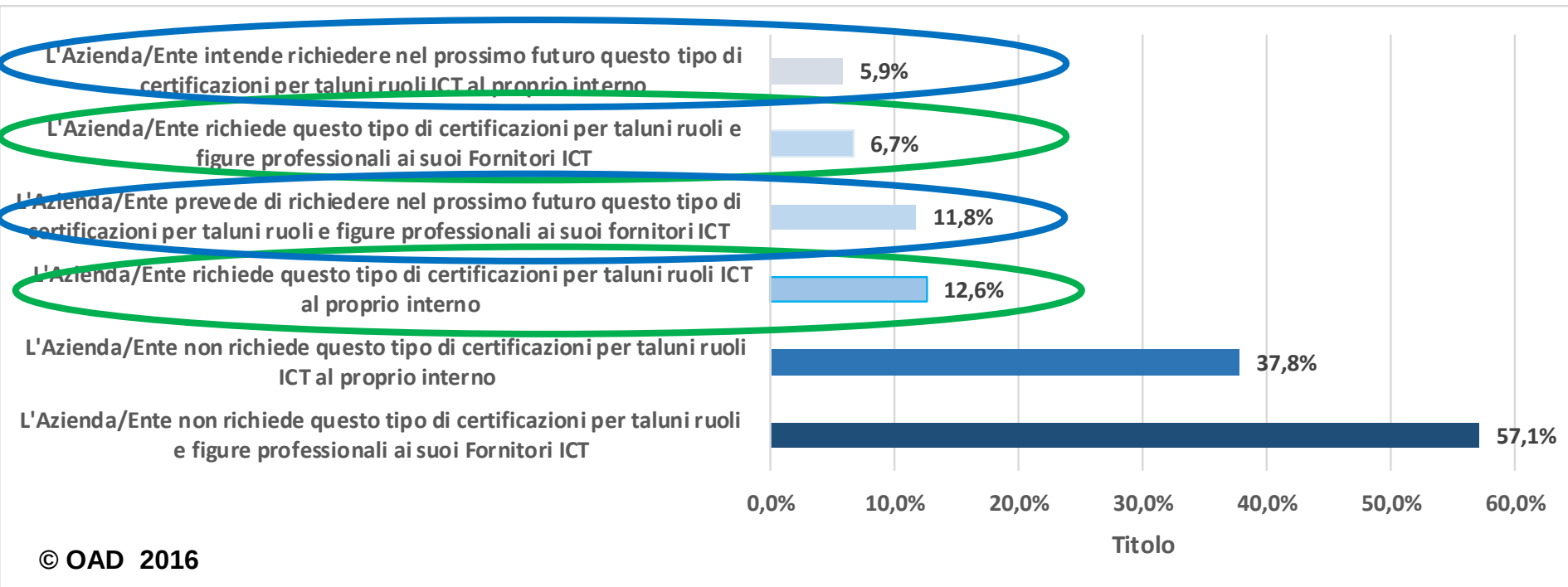
Livello di affidabilità del sistema informatico e/o di sue parti (risposte multiple)



I Sistemi Operativi in uso (risposte multiple)



Si richiedono certificazioni sulla sicurezza digitale? (risposte multiple)



Perché fare riferimento alle certificazioni eCF?

- Il sostanziale valore aggiunto della certificazione e-CF (UNI 11506, CEN 16234) è indicato nei seguenti punti
 - **ha valore giuridico** in Italia e in Europa (se erogata da una associazione registrata presso il MISE)
 - può valorizzare alcune altre **certificazioni indipendenti**
 - si basa sulla **provata esperienza** maturata sul campo dal professionista
 - qualifica il professionista considerando **l'intera sua biografia professionale** e le competenze ed esperienze maturate nella sua vita professionale (e non solo per aver seguito un corso e superato un esame)
-
- La strada è in salita ...
 - La certificazione eCFPlus per la reale qualificazione del professionista è un elemento basilare nell'ambito degli **obiettivi di AIPSI per la crescita professionale dei suoi Soci**

Riferimenti

m.bozzetti@aipsi.org

www.aipsi.org

www.issa.org

www.malaboadvisoring.it

www.nextvalue.it

