Milano, 9 maggio 2017

# *Dall'indagine OAD 2017 sugli attacchi agli applicativi in Italia.*

**Marco R.A. Bozzetti**

***Presidente AIPSI***

***Ideatore e curatore OAD***

***CEO Malabo Srl***

# Workshop del 9/5/2017

## *Attacchi agli applicativi informatici: la situazione in Italia*

- Marco R. A. Bozzetti, AIPSI e Malabo : ***Dall'indagine OAD 2017 sugli attacchi agli applicativi in Italia***
- Paolo Arcagni, Italy F5 Networks: ***Sicurezza applicativa senza compromessi***
- Giovanni Zanetti, AIPSI e Ericsson: ***Esempi ed esperienze di casi reali***
- Giuseppe Pontin, Nestlé Italy Group: ***Esempi ed esperienze di casi reali***

aipsi
ASSOCIAZIONE ITALIANA PROFESSIONISTI SICUREZZA INFORMATICA

# AIPSI
# e
# l'iniziativa OAD

OAD
Osservatorio
Attacchi Digitali
in Italia

# 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 nella crescita 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, 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**

- ***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**
  - **Rigoroso anonimato per i rispondenti ai questionari**
  - **Collaborazione con numerose associazioni (Patrocinatori) per ampliare il bacino dei rispondenti e dei lettori**

OsservatoriO AttacchInformatici

OAD
Osservatorio Attacchi Digitali in Italia

# Le precedenti edizioni OAD-OAI


**Scaricabili da**

**http://www.aipsi.org/**

**http://www.malaboadvisoring.it/**

# Sponsorizzazioni e patrocini OAD 2017 Attacchi Applicativi

## Sponsor Gold

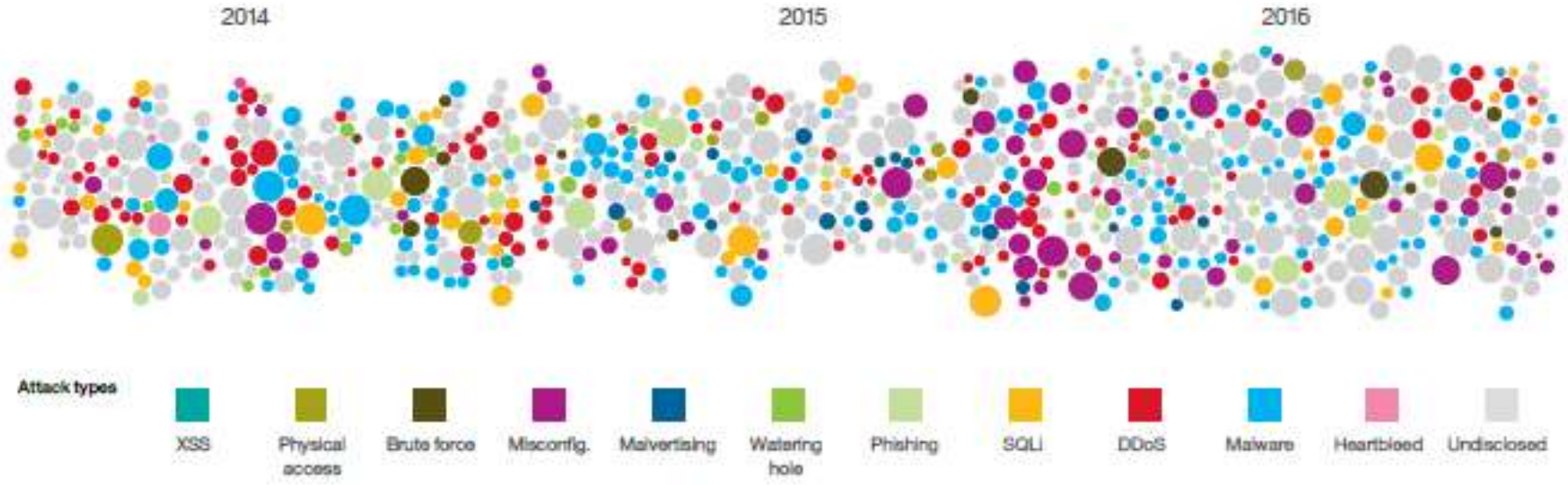
## Patrocinatori

## Le risposte al Questionario 2017 sugli attacchi agli applicativi

- Questionario online via web con 14 domande e risposte da selezionare con un click tra quelle predefinite
- Risposte completamente anonime
- Coinvolti potenziali rispondenti dalle mailing list di AIPSI, di Malabo, di Reportec e dei Patrocinatori
- 173 rispondenti al questionario

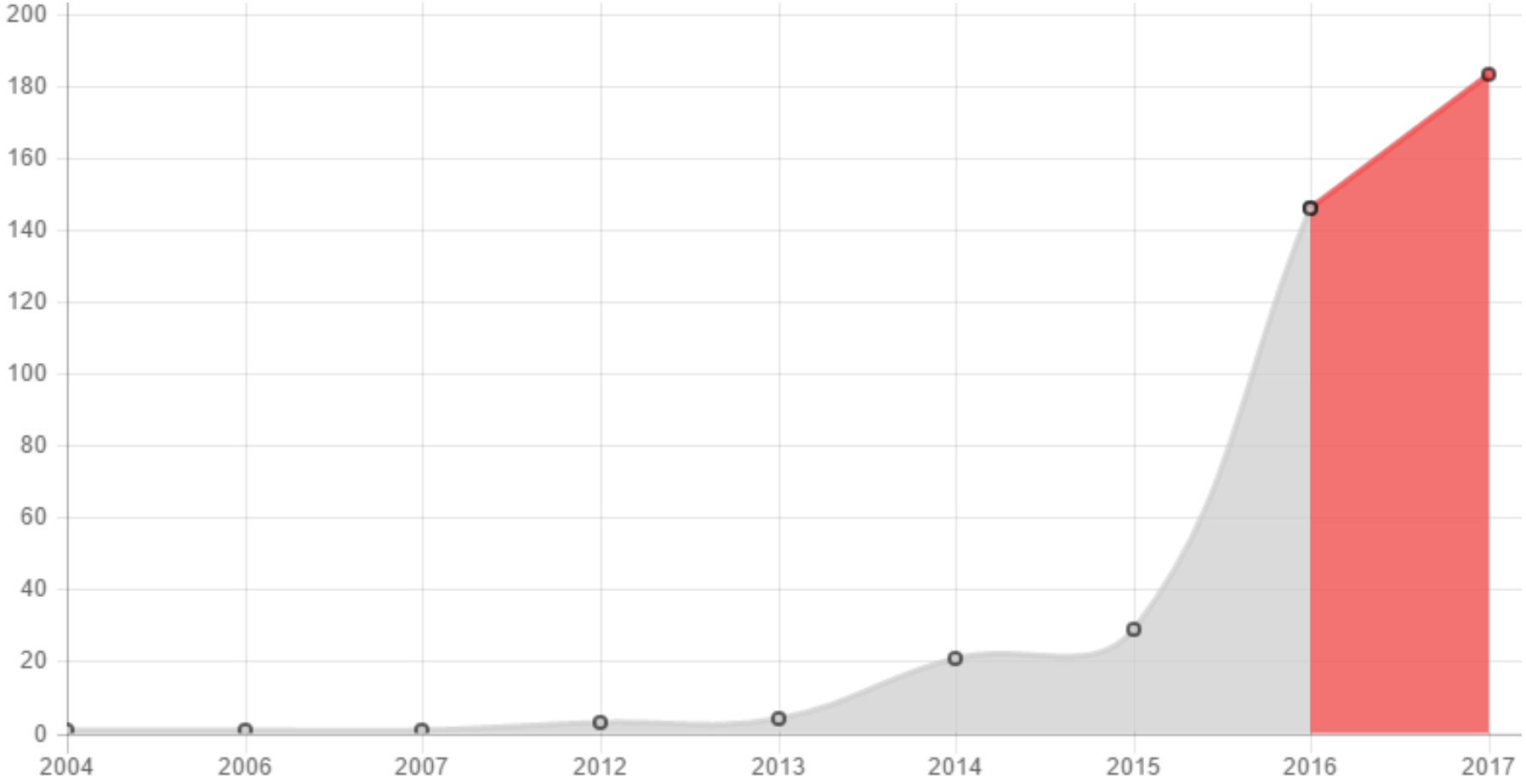
# Attacchi e vulnerabilità

# Panoramica attacchi 2014-16
# a livello mondiale per tipo e durata



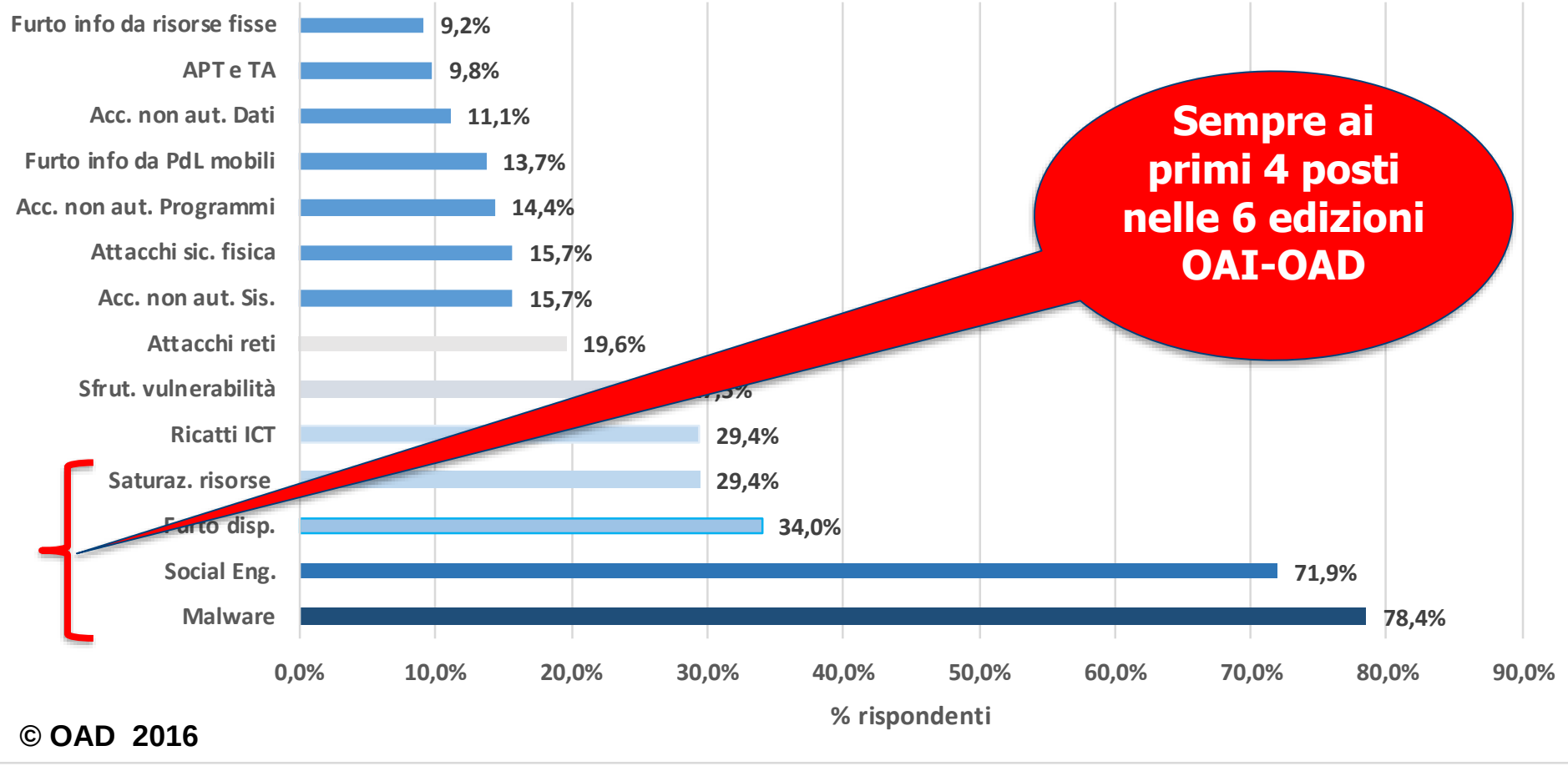

Fonte: IBM Xforce, marzo 2017

# La crescita del ransomware a livello mondiale

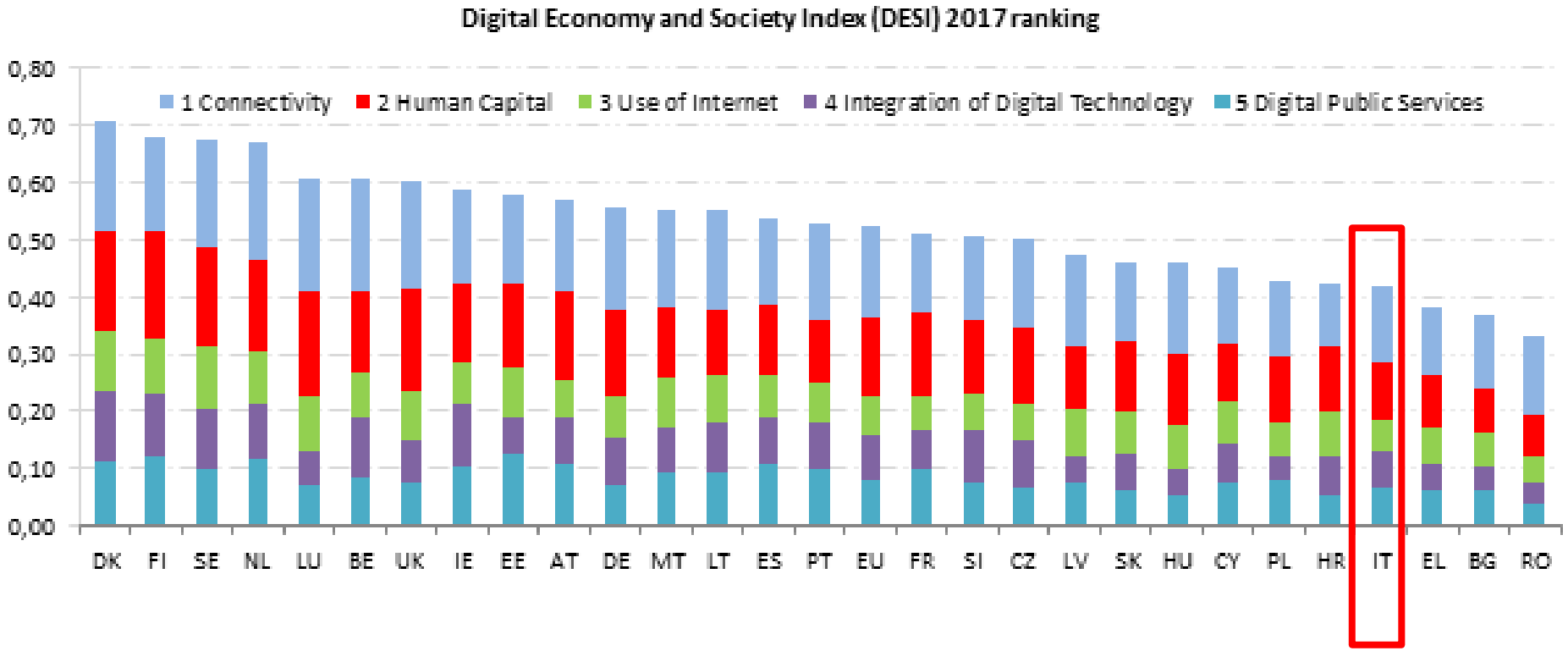



Fonte: TrendMicro

# OAD 2016: ripartizione percentuale per tipologia di attacco (risposte multiple)

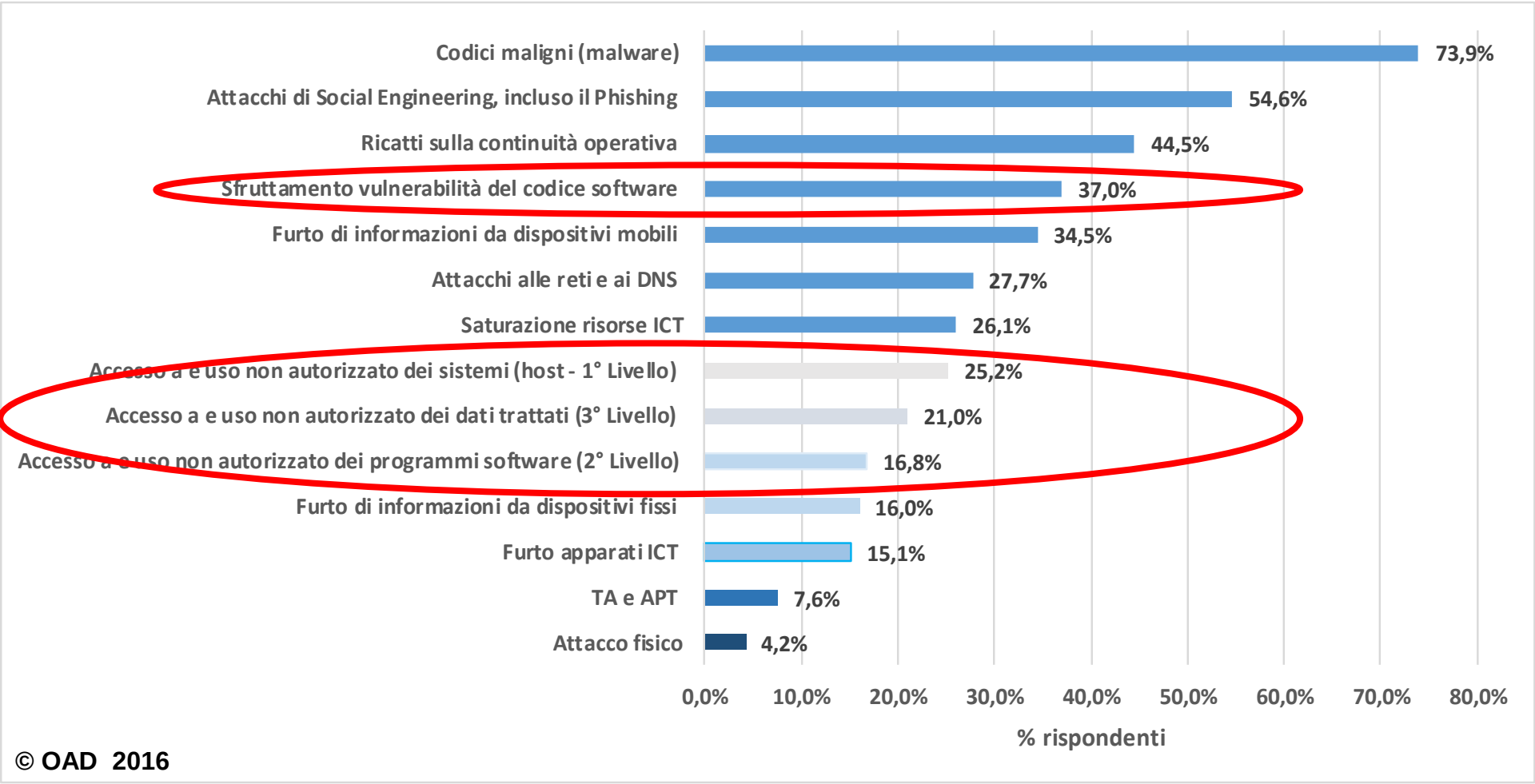


# Indice DESI europeo 2017 della digitalizzazione per nazione




Fonte: Comunità europea , marzo 2017

# OAD 2016: Quali gli attacchi più temuti nel prossimo futuro? (risposte multiple)



# Gli attacchi intenzionali agli applicativi dipendono da vulnerabilità dei sistemi ICT e … dagli esseri umani

- Degli applicativi
- Dei software di base - middleware
- Delle configurazioni e dei settaggi delle opzioni
- Delle architetture ICT
- Del comportamento degli utenti finali e degli amministratori di sistema

# Top Ten Vulnerabilità 2017 applicazioni web OWASP (Open Web Application Security Project)

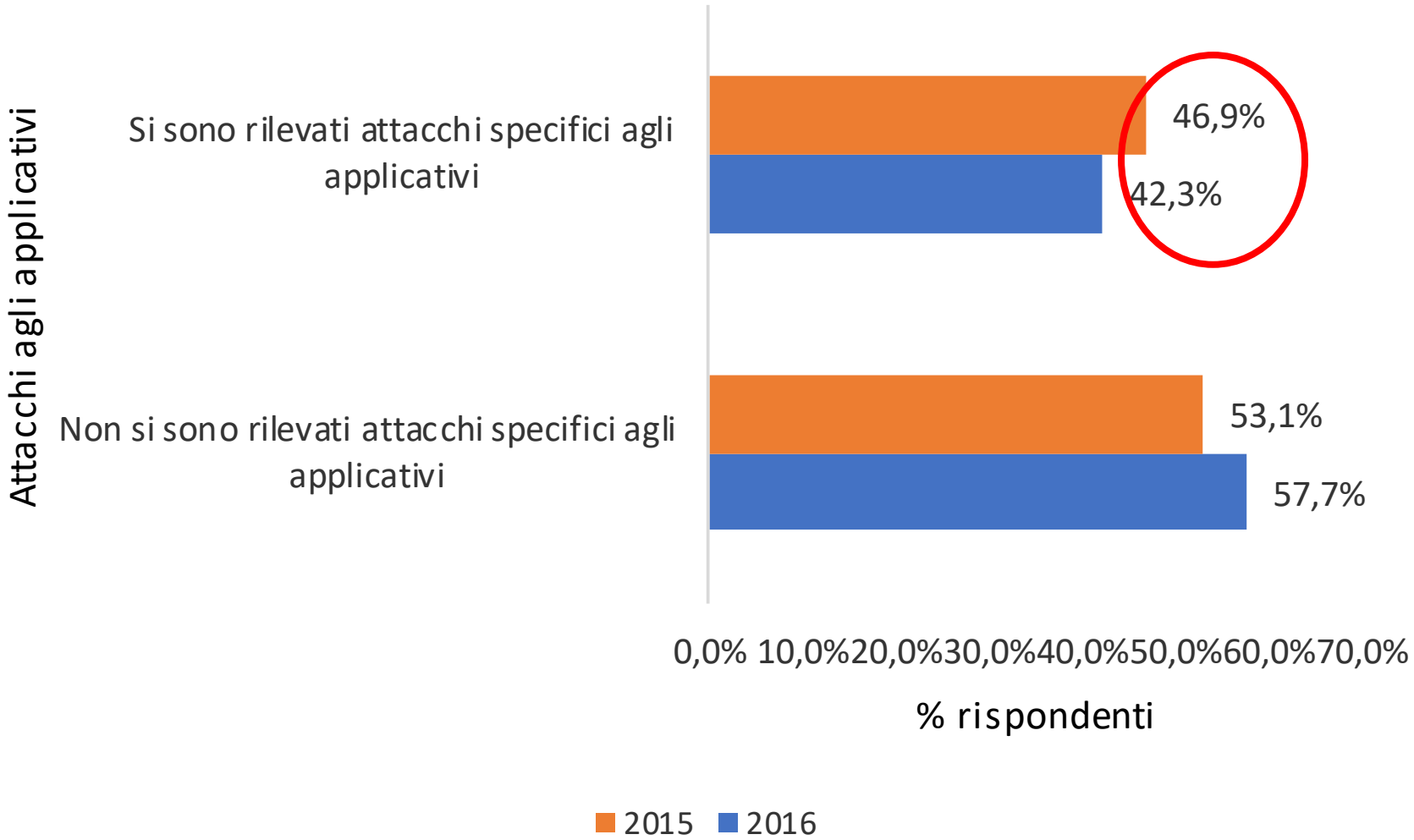
- Injection
- Broken Authentication and Session Management
- Cross-Site Scripting (XSS)
- Broken Access Control
- Security Misconfiguration
- Sensitive Data Exposure
- Insufficient Attack Protection
- Cross-Site Request Forgery (CSRF)
- Using Components with Known Vulnerabilities
- Underprotected APIs

# DB CVE: Numero di vulnerabilità indipendenti per tipo di prodotto (aprile 2017)

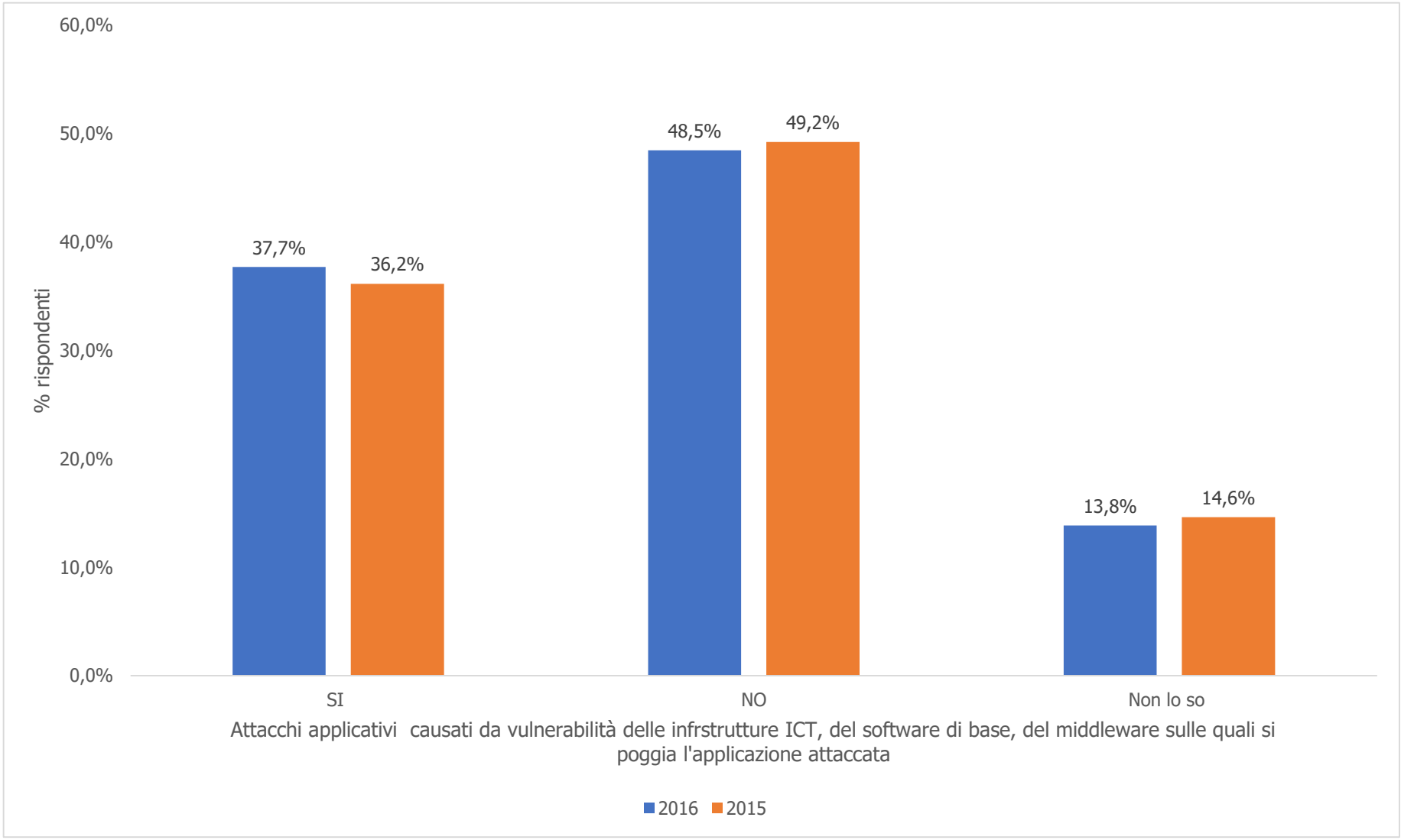
| | Nome del prodotto | Azienda | Tipo prodotto | Numero vulnerabilità individuate |
|---|---|---|---|---|
| 1 | Mac Os X | Apple | OS | 1820 |
| 2 | Linux Kernel | Linux | OS | 1815 |
| 3 | Firefox | Mozilla | Application | 1437 |
| 4 | Chrome | Google | Application | 1425 |
| 5 | Iphone Os | Apple | OS | 1176 |
| 6 | Flash Player | Adobe | Application | 1013 |
| 7 | Debian Linux | Debian | OS | 1003 |
| 8 | Android | Google | OS | 884 |
| 9 | Windows Server 2008 | Microsoft | OS | 846 |
| 10 | Safari | Apple | Application | 841 |
| 11 | Internet Explorer | Microsoft | Application | 840 |
| 12 | Ubuntu Linux | Canonical | OS | 839 |
| 13 | Windows Vista | Microsoft | OS | 814 |
| 14 | Opensuse | Novell | OS | 785 |
| 15 | Acrobat | Adobe | Application | 781 |
| 16 | Windows Xp | Microsoft | OS | 726 |
| 17 | Windows 7 | Microsoft | OS | 708 |
| 18 | Thunderbird | Mozilla | Application | 703 |
| 19 | Seamonkey | Mozilla | Application | 698 |
| 20 | Mac Os X Server | Apple | OS | 641 |

# OAD 2017 AA
# Attacchi
# agli applicativi
# rilevati

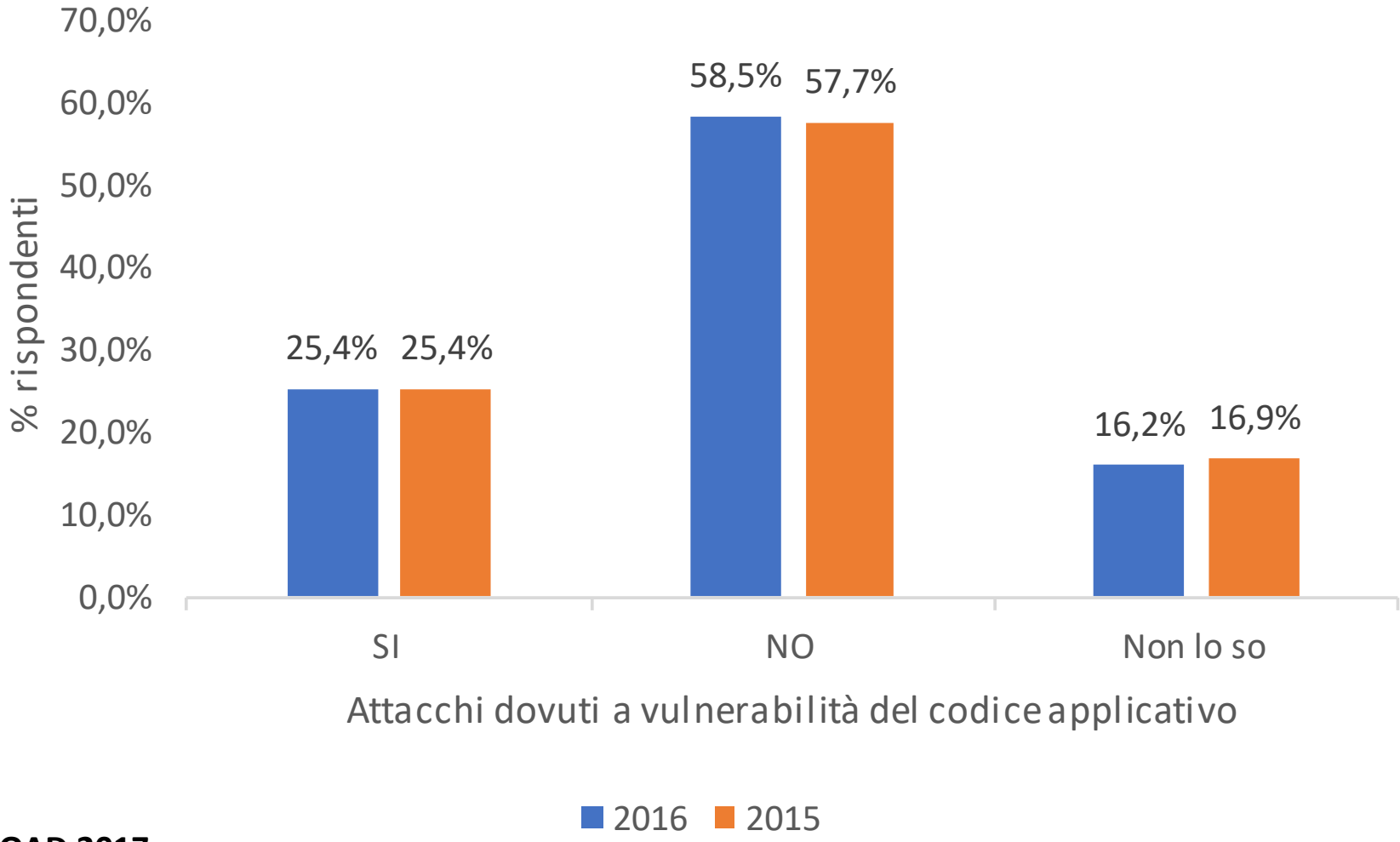
# OAD AA 2017: Attacchi agli applicativi rilevati



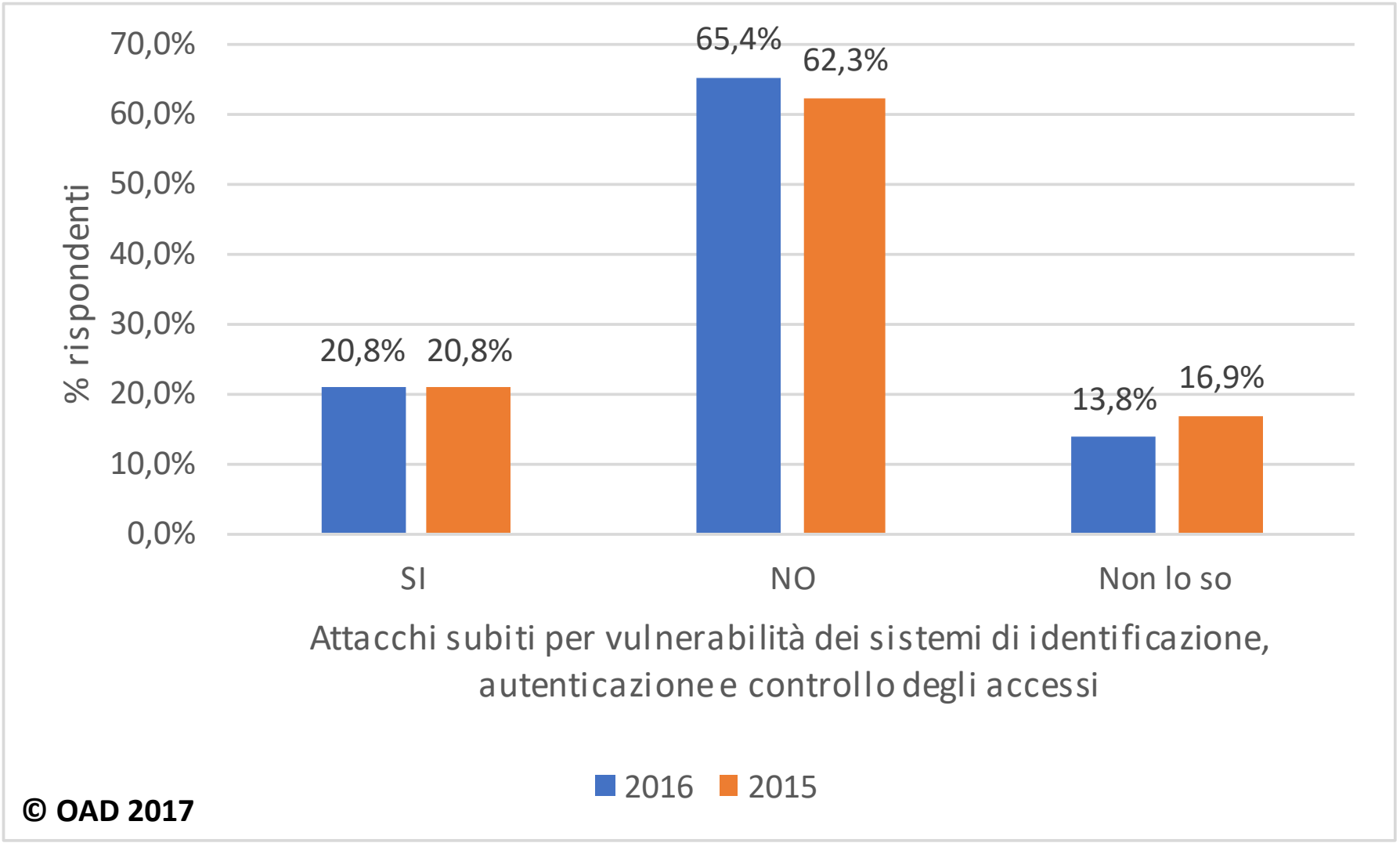
# OAD AA 2017: Attacchi dovuti alle vulnerabilità del software di base e del middleware



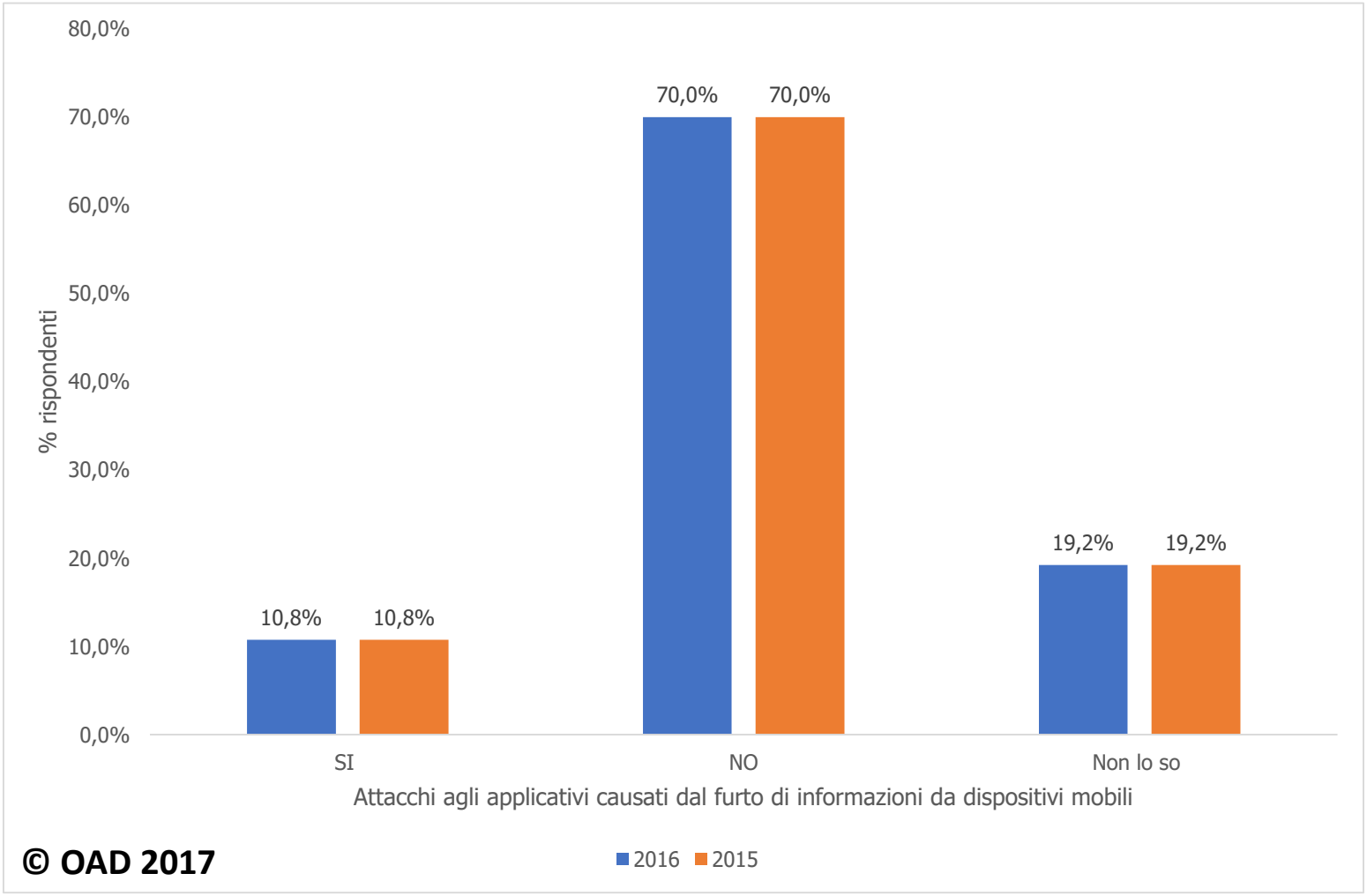
# OAD AA 2017: Attacchi dovuti a vulnerabilità del codice applicativo



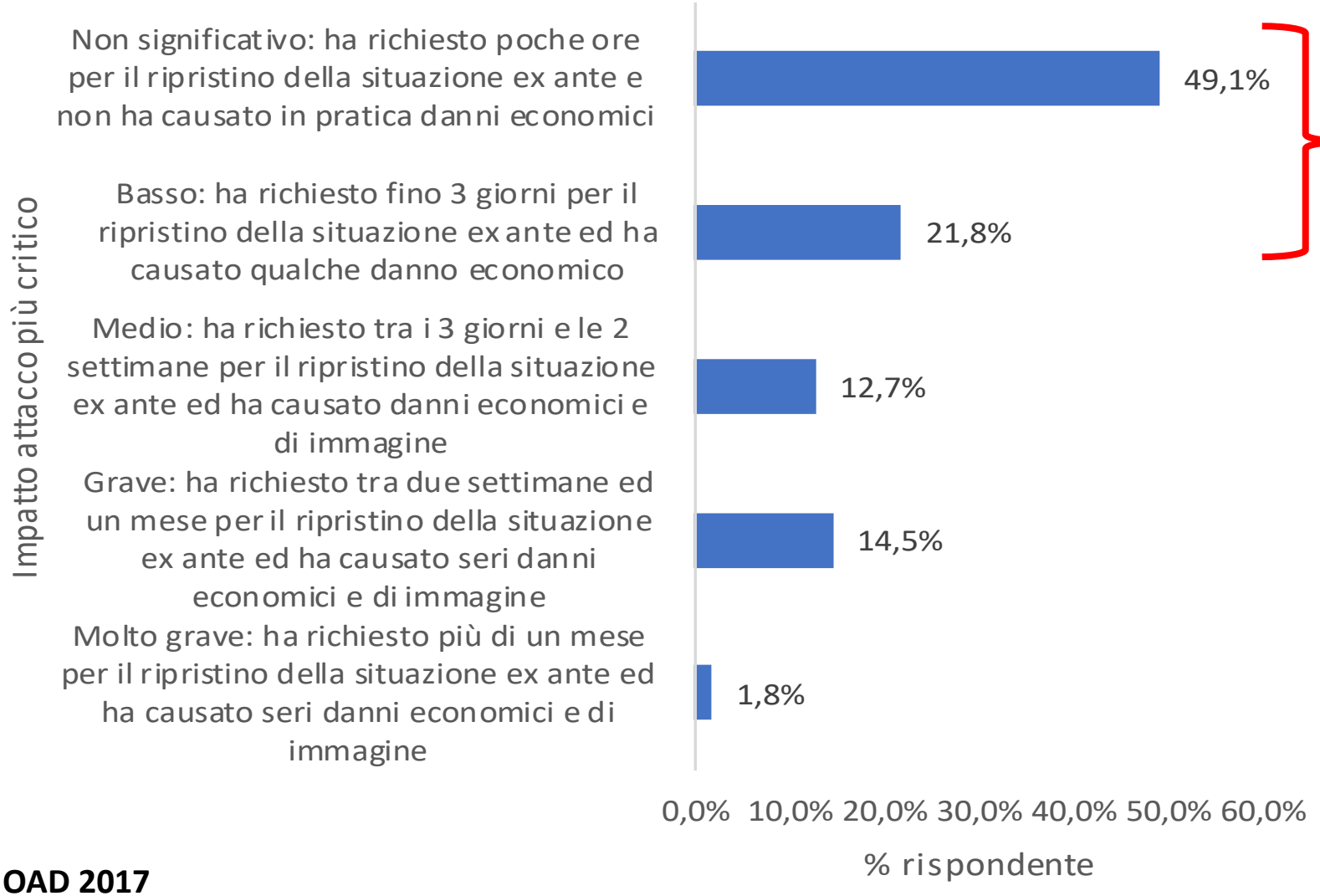
# OAD AA 2017: Attacchi per vulnerabilità identificazione-autenticazione-controllo accessi



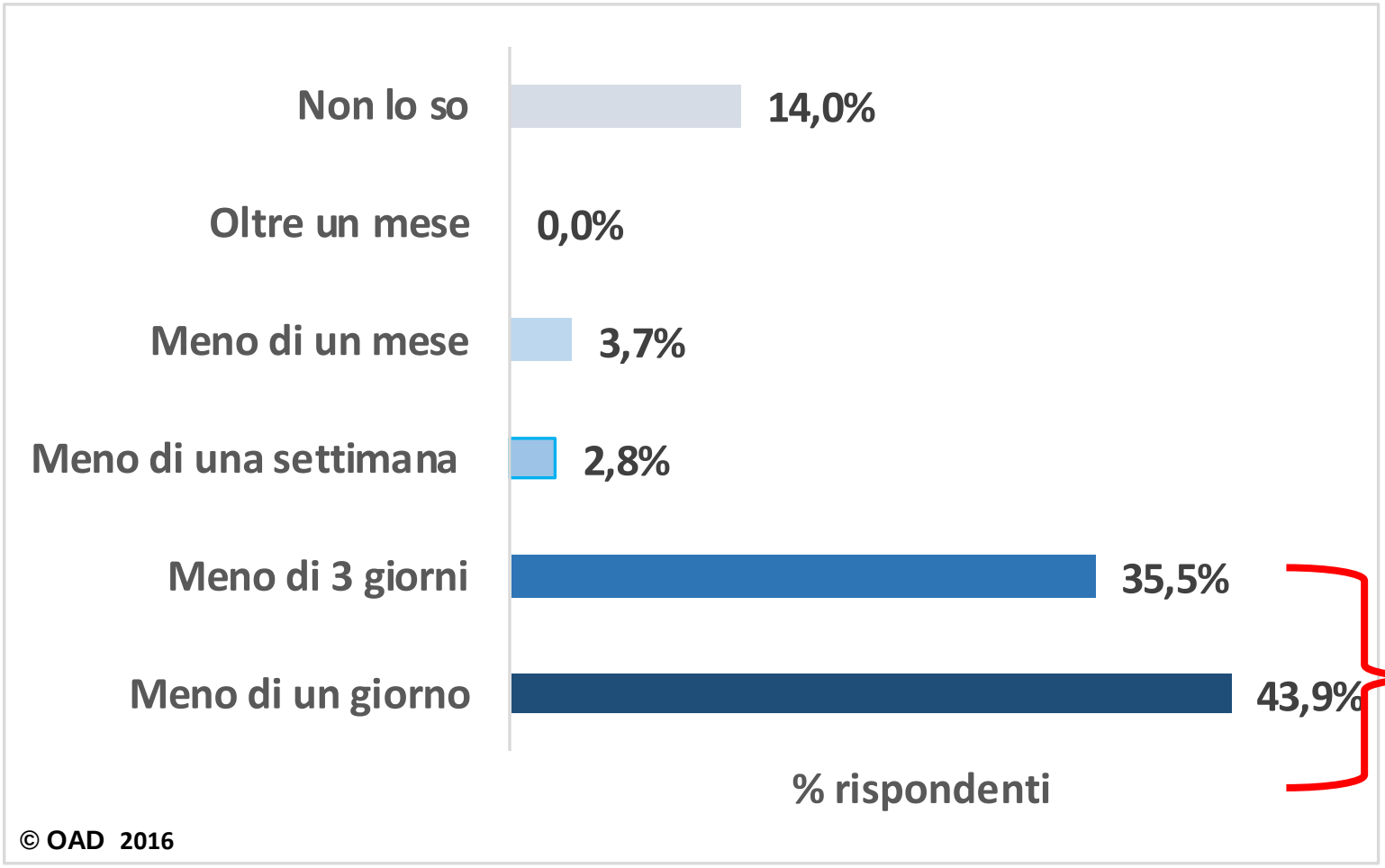
# OAD AA 2017: Attacchi dovuti al furto di informazioni da dispositivi mobili



# OAD AA 2017: Impatto dell'attacco peggiore come tempo ripristino

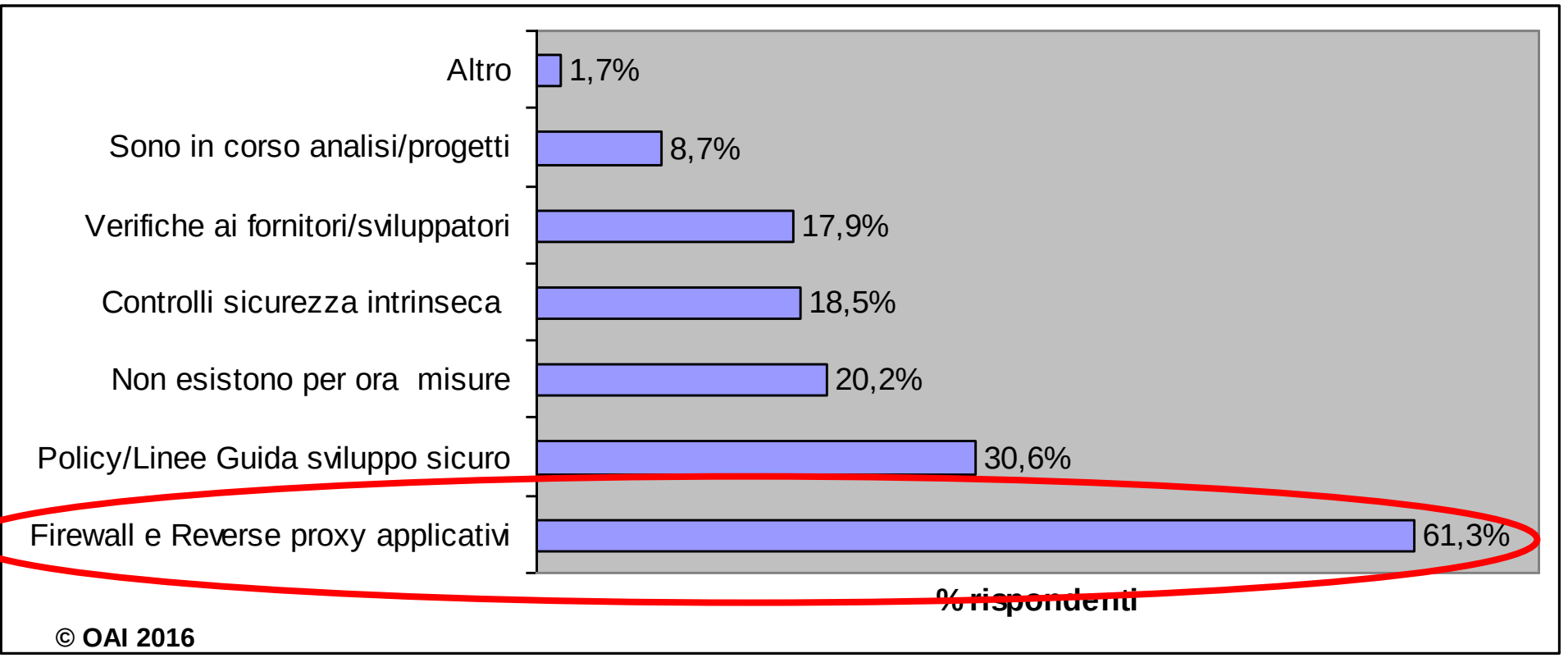


# OAD 2016: Tempo massimo occorso per il ripristino dei sistemi ICT

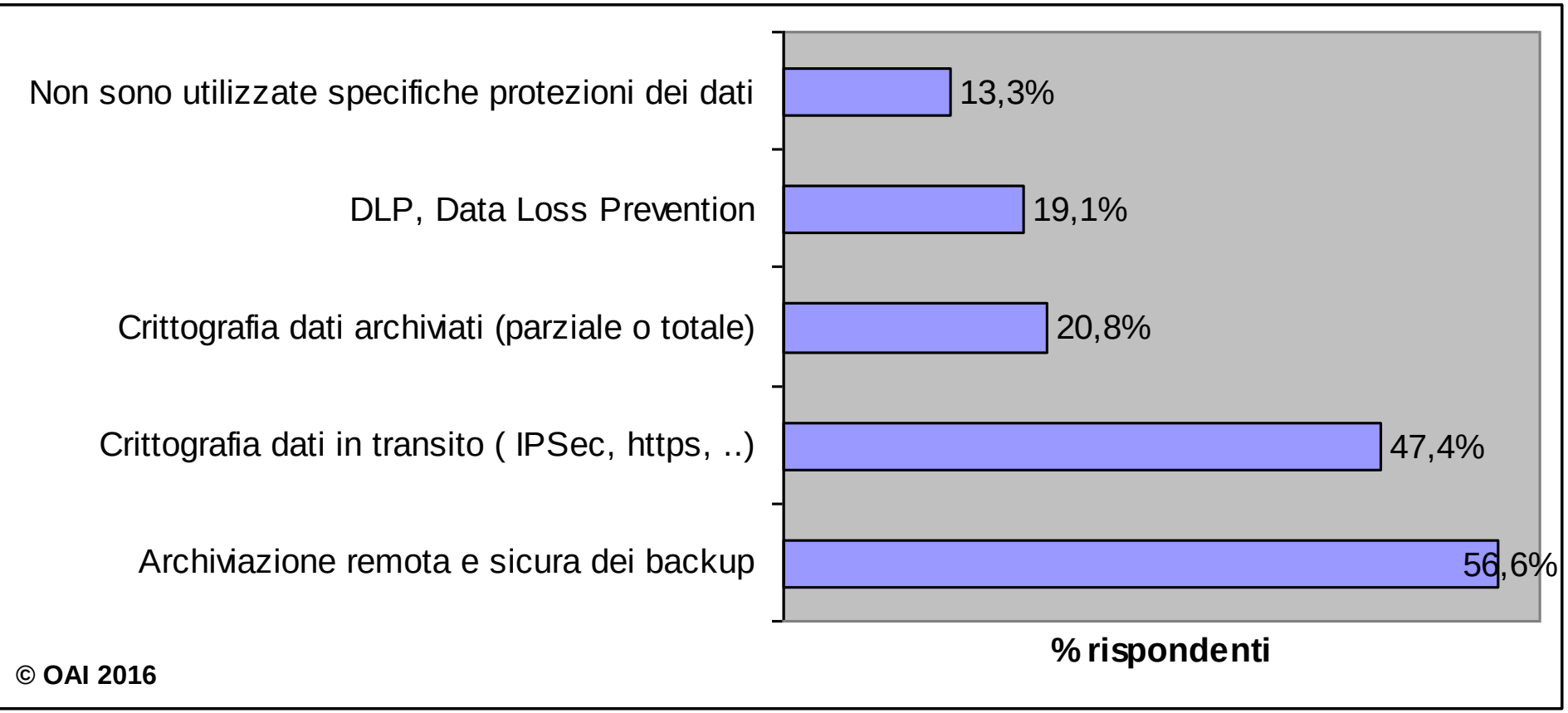


# OAD 2017 AA
# Le misure di sicurezza in essere

# OAD 2016: Misure di sicurezza per l'ambito applicativo (risposte multiple)



# OAD 2016: Strumenti in uso per la sicurezza logica delle informazioni (risposte multiple)

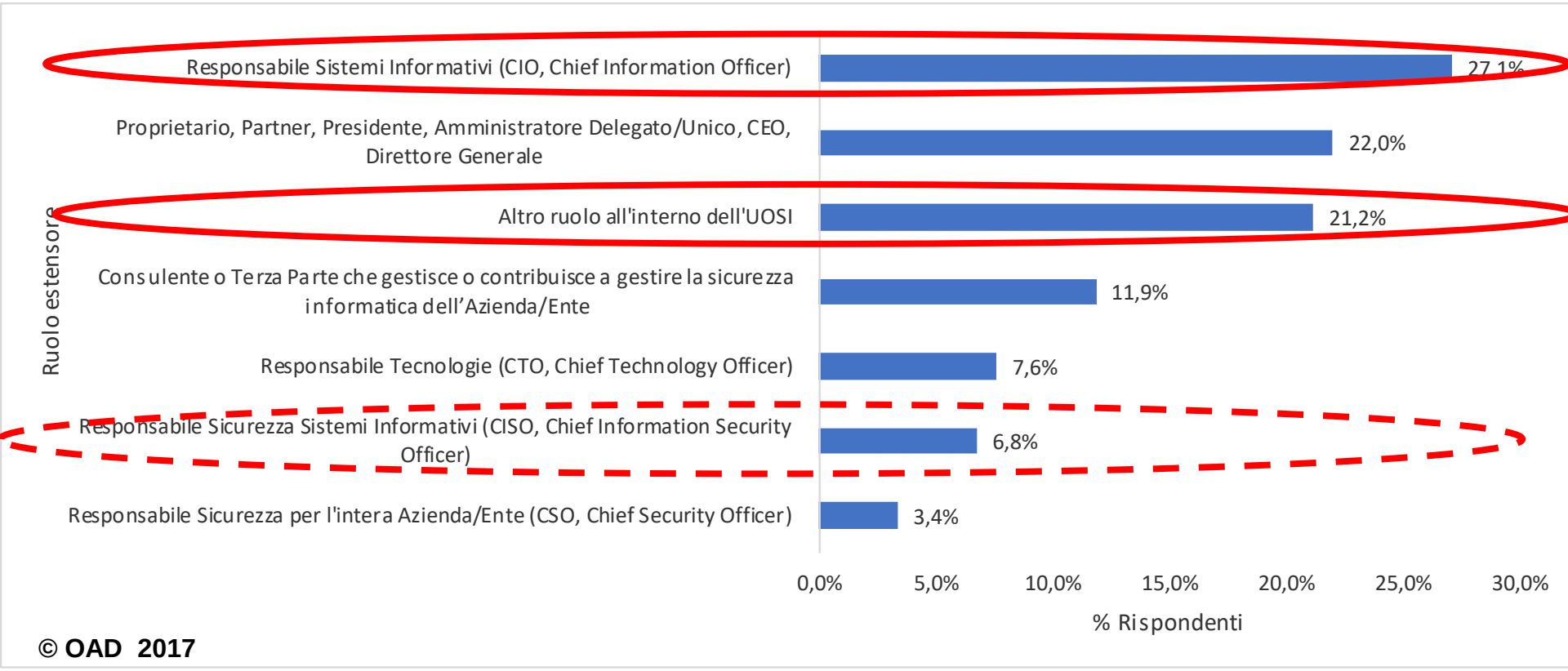


# OAD AA 2017: Misure di sicurezza per gli applicativi indagate (risposte multiple)

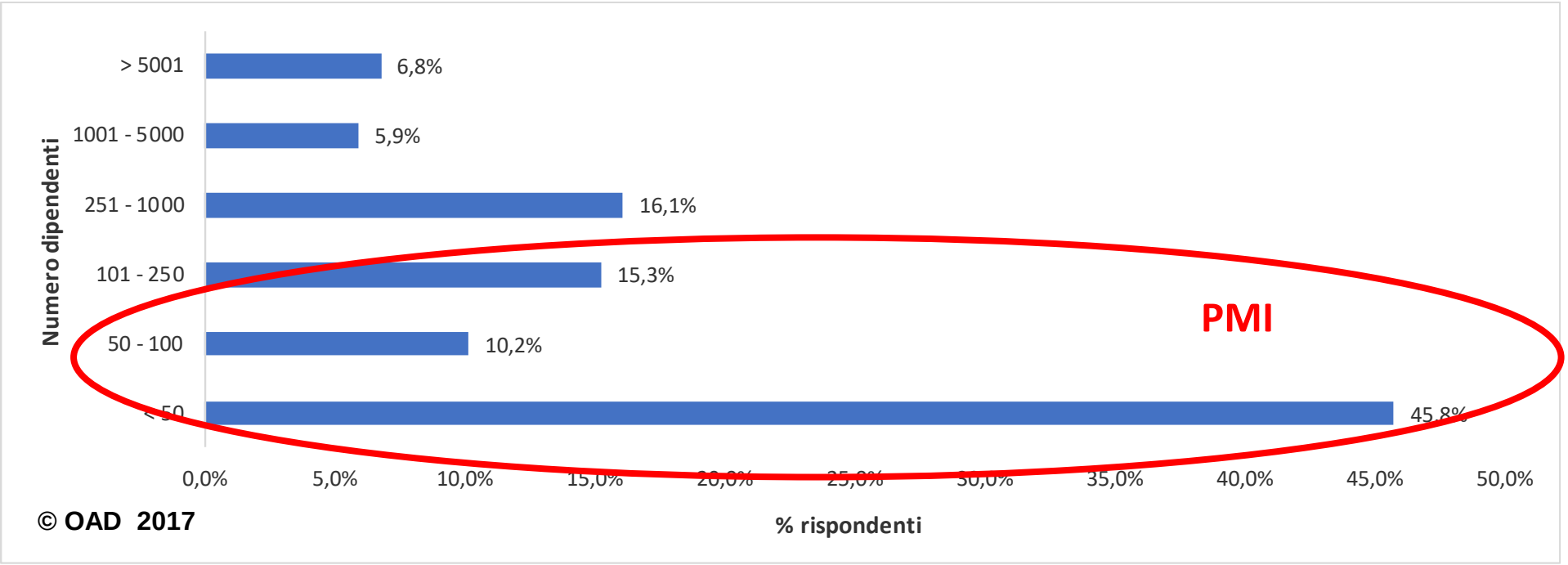
- Classificazione delle applicazioni per la criticità dei dati trattati → 70 %
- Centralizzazione IAM e Controllo Accessi → 84%
- Test tecnici e sicurezza intrinseca applicazione → 69%
- Penetration test → 55%

# OAD 2017 AA
# Il campione emerso
# ed il suo contesto applicativo

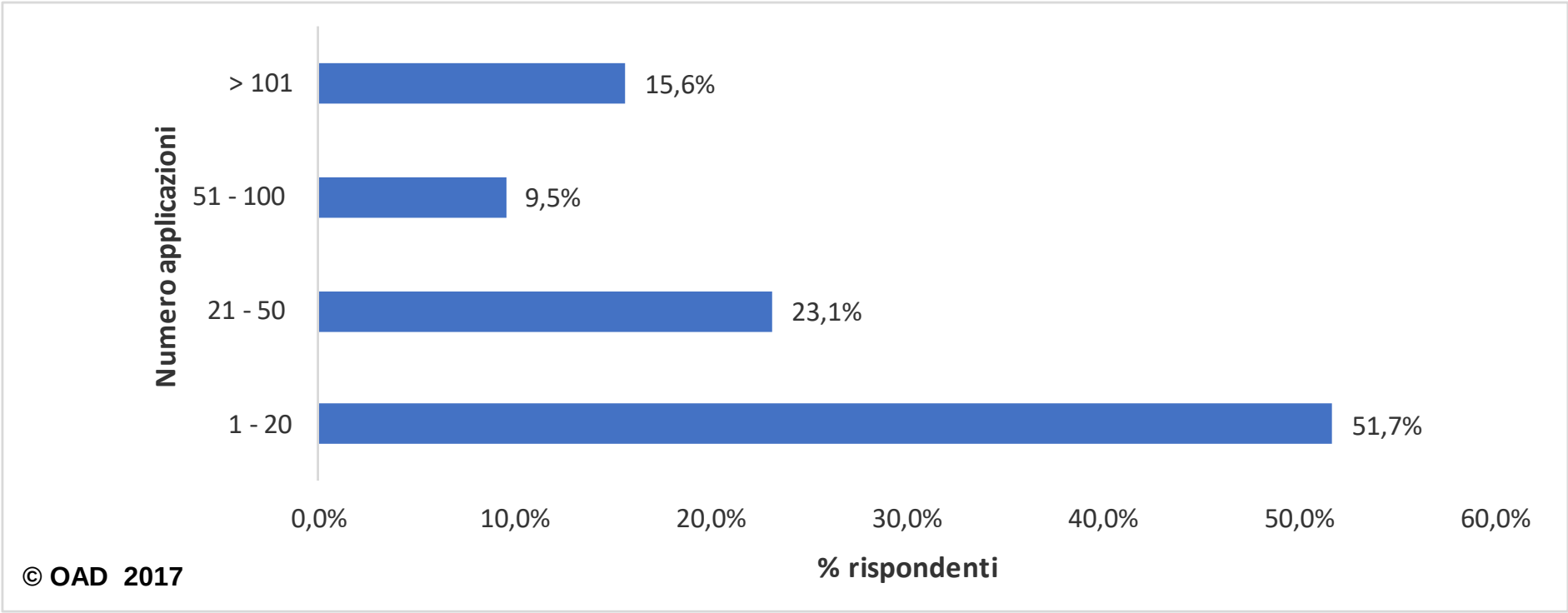
# OAD 2017 AA: Ruolo dei rispondenti



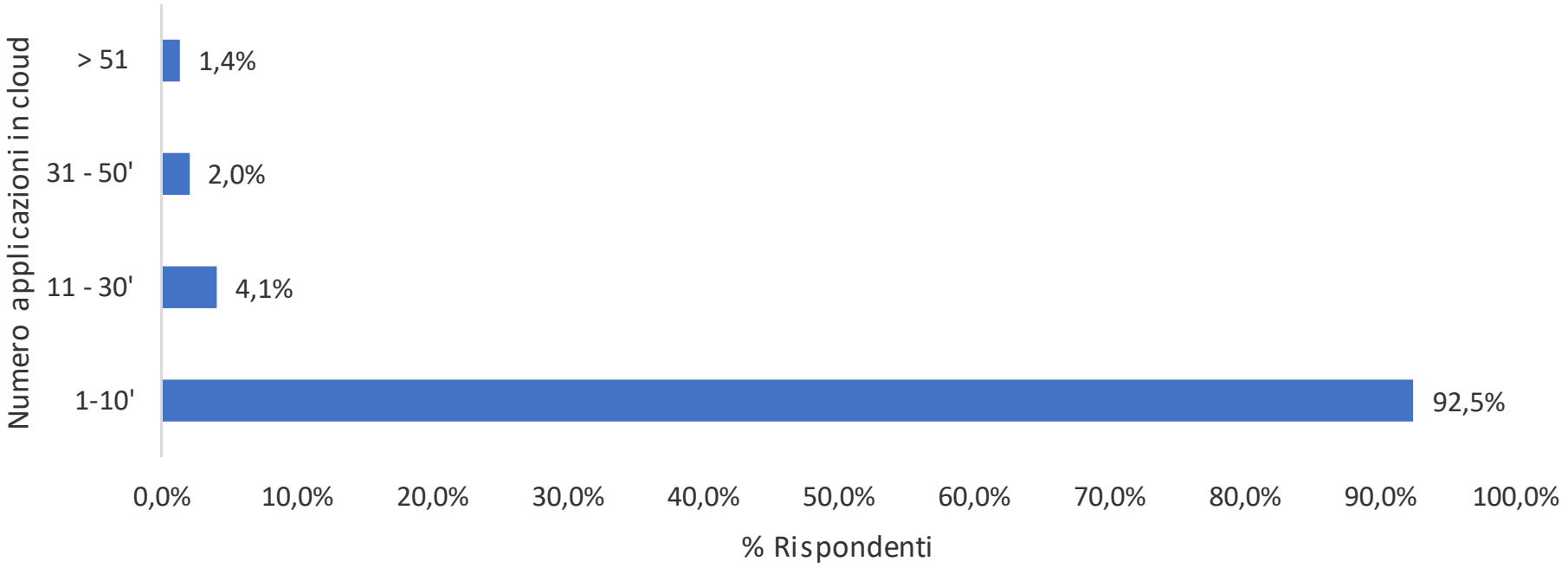
# OAD 2017 AA: Dimensioni aziende/enti dei rispondenti per numero di dipendenti



# OAD 2017 AA: numero applicazioni nel SI



# OAD 2017 AA: Numero applicazioni in cloud



# Riferimenti

m.bozzetti@aipsi.org

www.aipsi.org

www.issa.org

www.malaboadvisoring.it