

**ICT!TRADE 2010**  
FERRARA FIERE 8 E 9 GIUGNO 2010

# L'iniziativa OAI e il Rapporto 2009

**Marco R.A. Bozzetti**  
Past President FidaInform e ClubTI Milano  
GeaLab Srl, Malabo Srl

# Indice

---

## ***1. L'iniziativa OAI, Osservatorio Attacchi Informatici in Italia***

1. Il Rapporto 2009

1. I prossimi passi per il Rapporto 2010

# OAI, Osservatorio Attacchi Informatici in Italia

---

- **Che cosa è**
  - Indagine annuale sugli attacchi ai Sistemi Informativi di Aziende e Pubbliche Amministrazioni in Italia condotta attraverso un questionario on-line indirizzato a CIO, CISO, CSO ed ai consulenti che si occupano di sicurezza informatica
- **Gli ideatori e realizzatori**



ClubTI Milano



La federazione dei ClubTI in Italia



L'Editore

# Federazione Italiana Delle Associazioni professionali per l'INFORmation Management



[www.fidainform.it](http://www.fidainform.it)

[www.clubtimilano.net](http://www.clubtimilano.net)

- La missione di FIDA è di garantire un contributo professionale di alto livello e con caratteristiche di “terzietà” nei processi conoscitivi e decisionali chiave dell’ICT italiana, al fine di valorizzare i propri soci, la professione ICT e di migliorare, con l’uso intelligente della tecnologia, la qualità della vita nel nostro Paese.

- I ClubTI, e quindi la loro Federazione FIDA, si propongono come «nodo» attivo del Sistema-Paese per lo sviluppo del Settore ICT “allargato”, promuovendo la professionalità dei Soci

- complessivamente > 1.000 associati
- Rivista bimestrale ICT Professional distribuita a 7000 “decision maker” e influenzatori dell’ICT



# Obiettivi OAI

---

- Avere cadenza periodica annuale
- Coinvolgere tutte le Associazioni e gli Enti coinvolti e/o interessati nella sicurezza informatica
- Divenire uno strumento di ausilio nell'Analisi del Rischio ed il **punto di riferimento nazionale sulla sicurezza ICT**, analogamente a quanto avviene con il Rapporto CSI statunitense
- Far conoscere e sensibilizzare i vertici delle Aziende/Enti sui problemi della sicurezza ICT
- Che cosa non è e non vuole essere OAI :
  - Un'indagine criminologica estesa a tutti i crimini informatici (es. pornografia e pedofilia elettronica, pirateria prodotti software, ecc.)
  - Uno studio accademico
  - Un'indagine di mercato

# Collaborazioni e patrocini Rapporto OAI 2009

---

## Con la collaborazione della Polizia delle Comunicazioni



### I patrocinatori

- Aipsa
- Aipsi
- Assolombarda
  - FTI
- Inforav



# Indice

---

## 1. L'iniziativa OAI, Osservatorio Attacchi Informatici in Italia

### *1. Il Rapporto 2009*

#### 1. I prossimi passi per il Rapporto 2010

# Il Rapporto OAI 2009

- In formato elettronico
  - Disponibile gratuitamente in vari siti web **previa registrazione**:
    - [www.aipsi.org](http://www.aipsi.org)
    - [www.clubtimilano.net](http://www.clubtimilano.net)
    - [www.fidainform.it](http://www.fidainform.it)
    - [www.forumti.it](http://www.forumti.it)
    - [www.malaboadvisoring.it](http://www.malaboadvisoring.it)
    - [www.soiel.it](http://www.soiel.it)
- Edizione cartacea



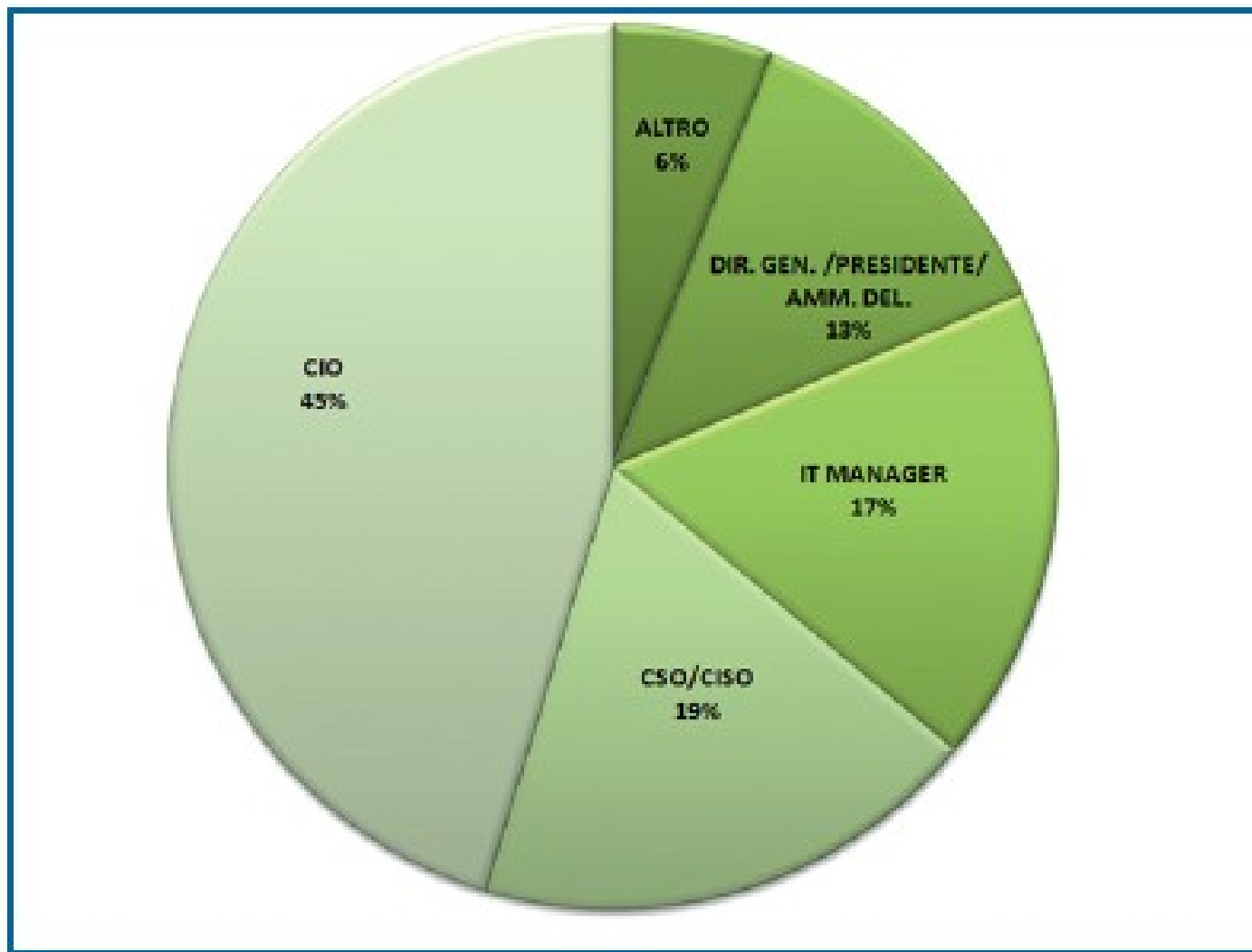
# La tassonomia degli attacchi considerata

---

- 1) **Accesso e uso non autorizzato** degli elaboratori, delle applicazioni supportate e delle relative informazioni
- 2) **Modifiche non autorizzate ai programmi** applicativi e di sistema, alle configurazioni ecc.
- 3) **Modifiche non autorizzate ai dati e alle informazioni**
- 4) Utilizzo **codici maligni** (malware) di varia natura, quali virus, Trojan horses, Rootkit, bots, exploits, sia a livello di posto di lavoro che di server
- 5) Utilizzo **vulnerabilità del codice software**, sia a livello di posto di lavoro che di server: tipici esempi back-door aperte, SQL injection, buffer overflow ecc.
- 6) **Saturazione risorse** informatiche e di telecomunicazione: oltre a DoS (Denial of Service) e DDoS (Distributed Denial of Service), si includono in questa classe anche mail bombing, catene di S. Antonio informatiche, spamming ecc.
- 7) **Furto di apparati** informatici contenenti dati (laptop, hard disk, floppy, nastri, chiavette USB ecc.)
- 8) **Furto di informazioni o uso illegale** di informazioni
  - a) da dispositivi mobili (palmari, cellulari, laptop)
  - b) da tutte le altre risorse
- 9) Attacchi alle **reti**, fisse o wireless, e ai **DNS**, Domain Name System
- 10) **Frodi** tramite uso improprio o manipolazioni non autorizzate e illegali del software applicativo (ad esempio utilizzo di software pirata, copie illegali di applicazioni ecc.)
- 11) Attacchi di **Social Engineering** e di **Phishing** per tentare di ottenere con l'inganno (via telefono, e-mail, chat ecc.) informazioni riservate quali credenziali di accesso e il furto d'identità digitale
- 12) **Ricatti** sulla continuità operativa e sull'integrità dei dati del sistema informativo (ad esempio se non paghi attacco il sistema e ti procuro danni, magari con dimostrazione delle capacità di attacco e di danno conseguente...)
- 13) Altri tipi di attacco, quali ad esempio **attacchi di tipo misto** (Blended threat), **sabotaggi**, **vandalismi** con distruzione di risorse informatiche.

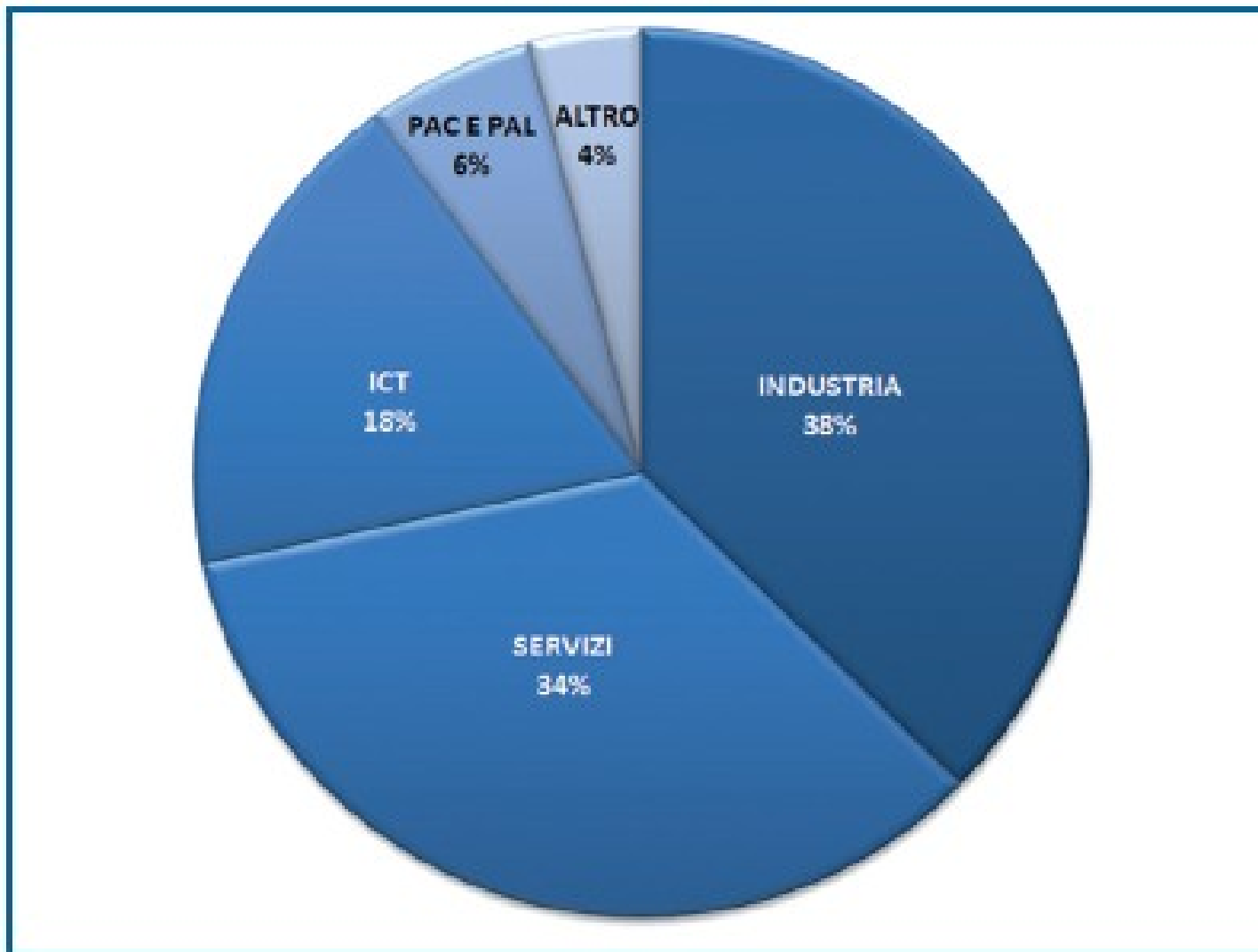
# OAI 2009: chi ha risposto al questionario (in %)

---



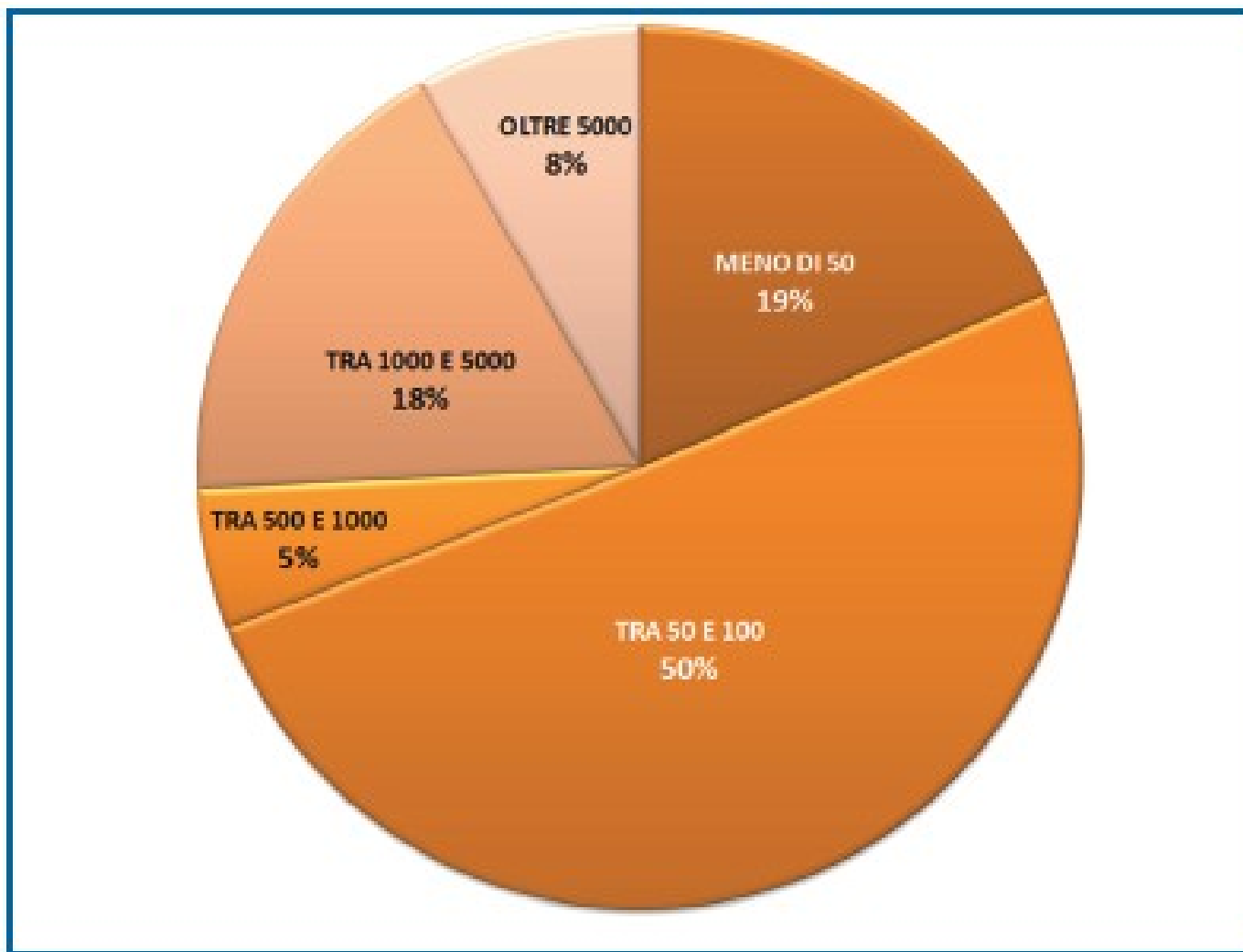
# OAI 2009: struttura merceologica del campione

---



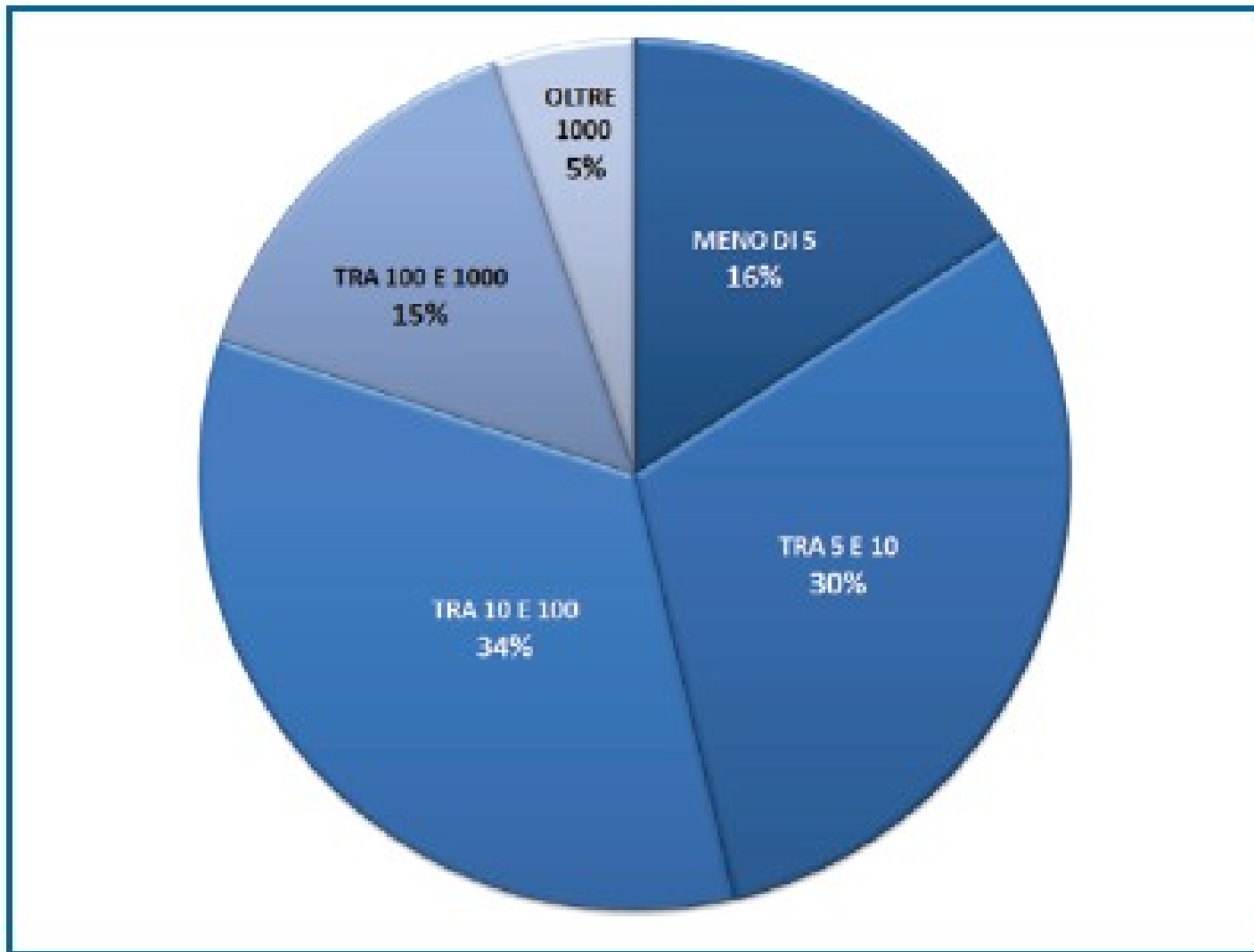
## OAI 2009: le dimensioni delle aziende del campione

---



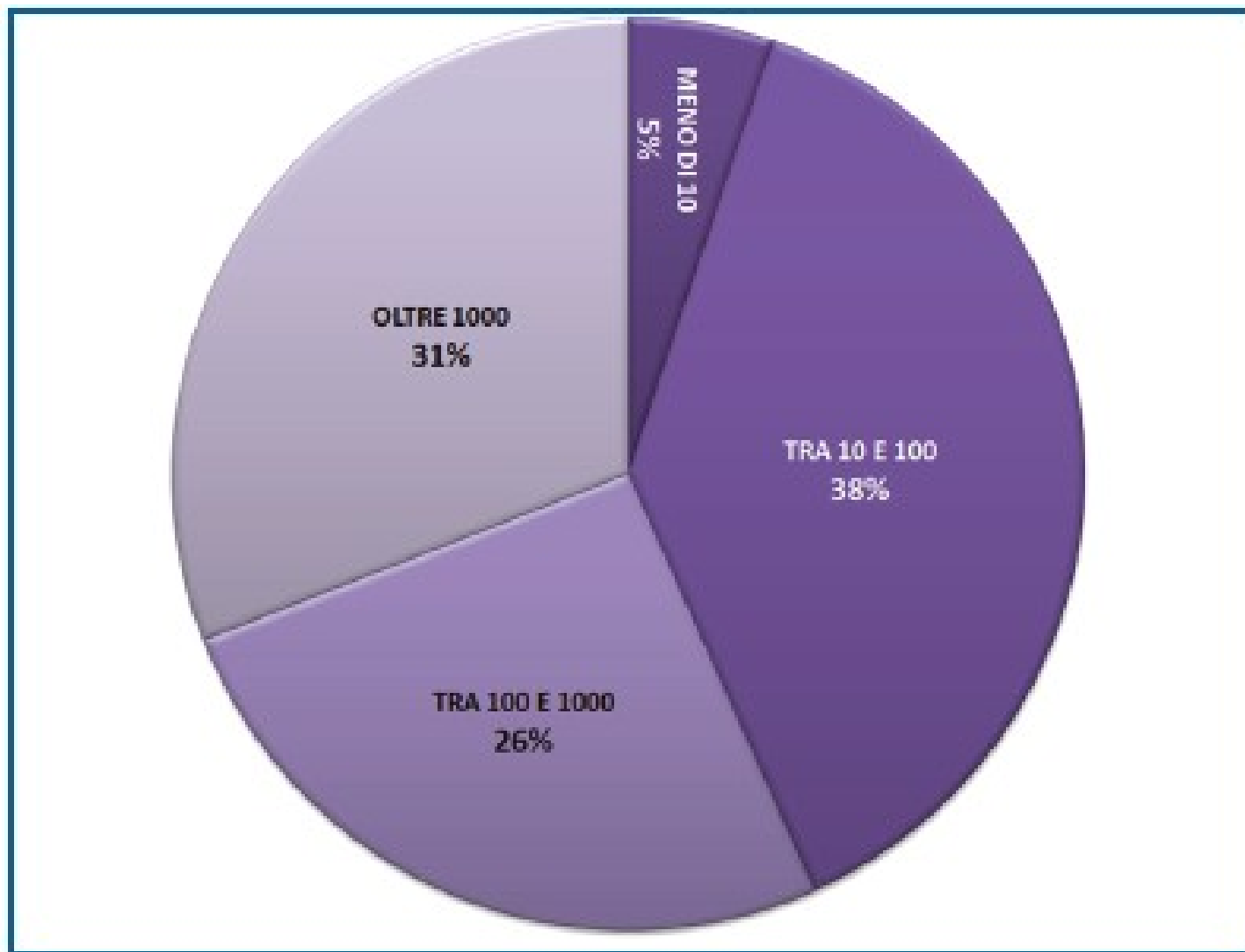
## OAI 2009: numero di server per sistema del campione

---



## OAI 2009: numero di posti di lavoro per sistema del campione

---



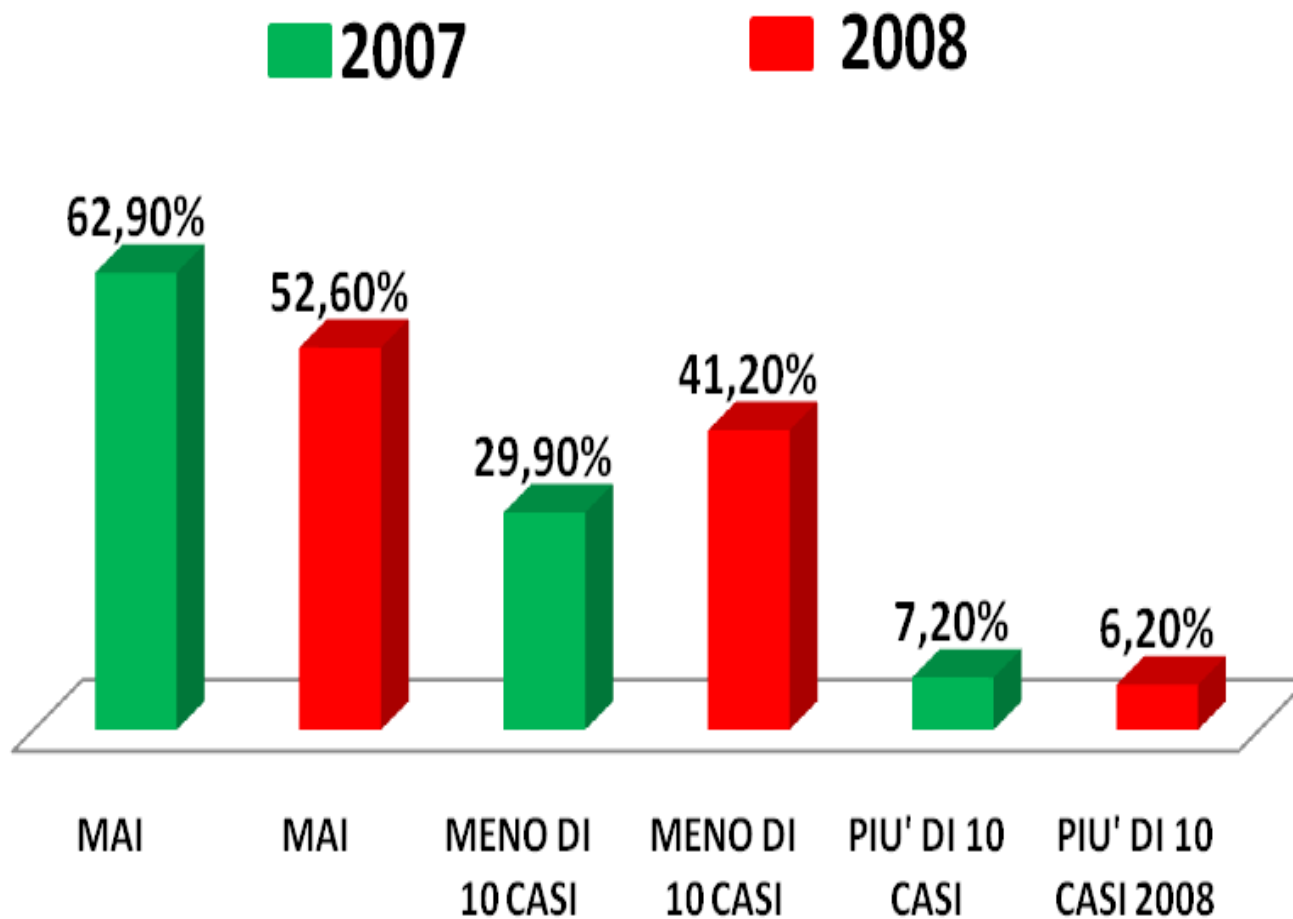
## OAI 2009: gestione diretta o terziarizzata (Data Center)

---

■ Data Center gestito internamente    ■ Data Center terziarizzato (in outsourcing)



# OAI 2009: % numero attacchi rilevati nel 2007 e nel 2008



## OAI 2009: attacchi più diffusi nel 2008

---

DIFFUSIONE ATTACCHI PER TIPOLOGIA 2008	COPERTURA (%)	GRADUATORIA
Utilizzo codici maligni (malware) sia a livello di posto di lavoro che di server	84%	1°
Attacchi di Social Engineering e di Phishing	58%	2°
Furto di apparati informatici contenenti dati (laptop, hard disk, floppy, nastri, chiavette)	50%	3°
Attacchi alle reti, fisse o wireless, e ai DNS (Domain Name System)	42%	4°
Accesso e ad uso non autorizzato degli elaboratori, delle applicazioni supportate e dei dati	34%	5°
Modifiche non autorizzate ai programmi applicativi e di sistema, alle configurazioni e ai dati	28%	6°
Frodi tramite uso improprio o manipolazioni non autorizzate e illegali del software applicativo	22%	7°

# OAI 2009: % strumenti in uso

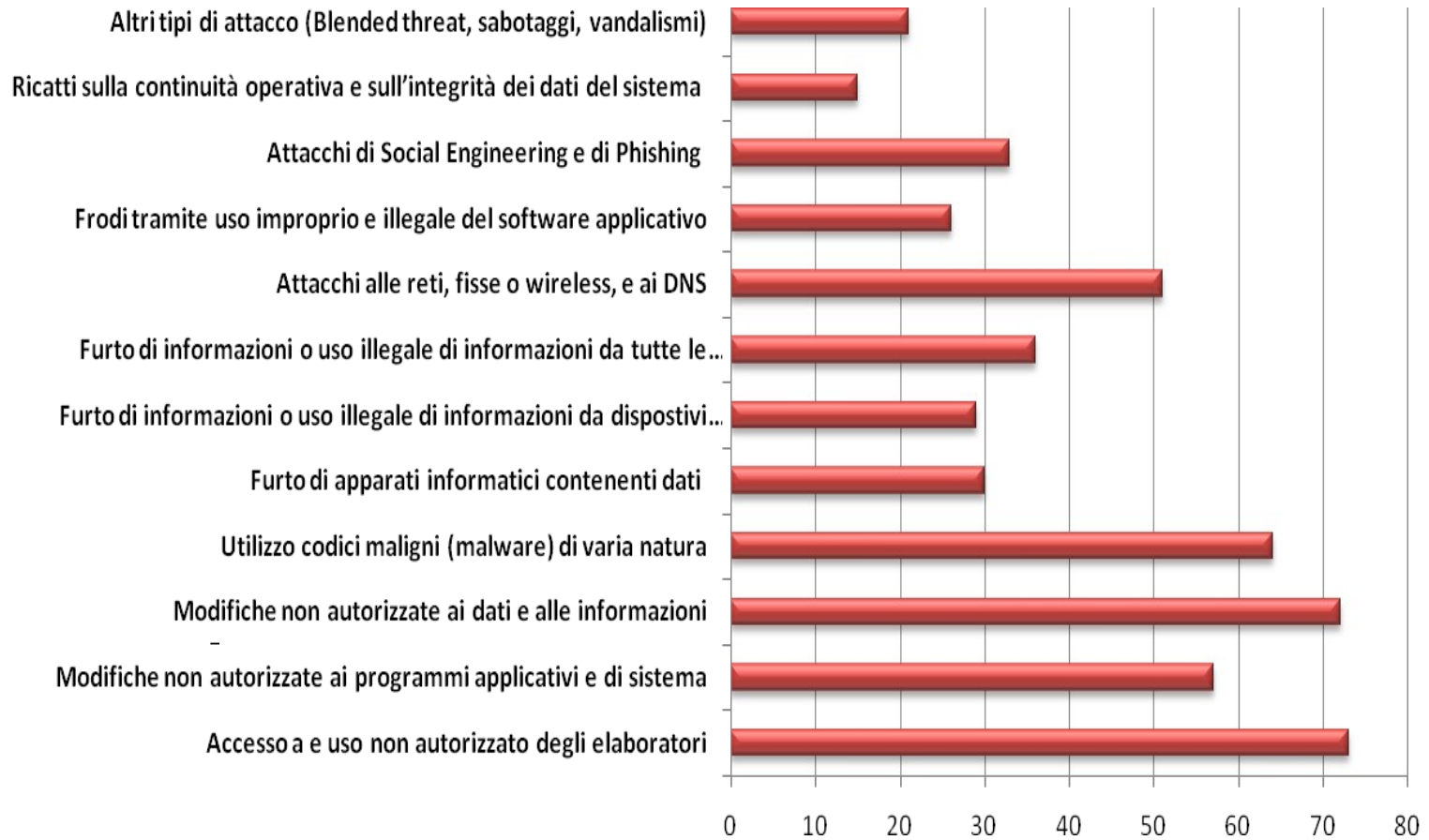
STRUMENTI E METODOLOGIE DI PROTEZIONE IN USO	%
Antivirus and antispymware	95%
Firewall e DMZ	85%
Identificazione dell'utente con identificativo d'utente e password	84%
VPN (Virtual Private Network)	79%
Strumenti di gestione delle autorizzazioni (Active Directory, Ldap, Access Control List, policy server)	77%
Uso di strumenti per la gestione delle patch, degli aggiornamenti, delle release	60%
Archiviazione e gestione dei log	52%
Politiche (policy) tecnico-organizzative di sicurezza ICT	52%
Uso sistemi ad alta affidabilità	47%
Disaster Recovery Planning	39%
Uso di procedure organizzative formalizzate nel supporto ai processi inerenti la sicurezza informatica	38%
Sistemi di PKI (Public Key Infrastructure)	20%
Identificazione dell'utente "forte" con certificati digitali	20%
Identificazione dell'utente biometrica	6%

# OAI 2009: l'analisi degli strumenti in uso per settore

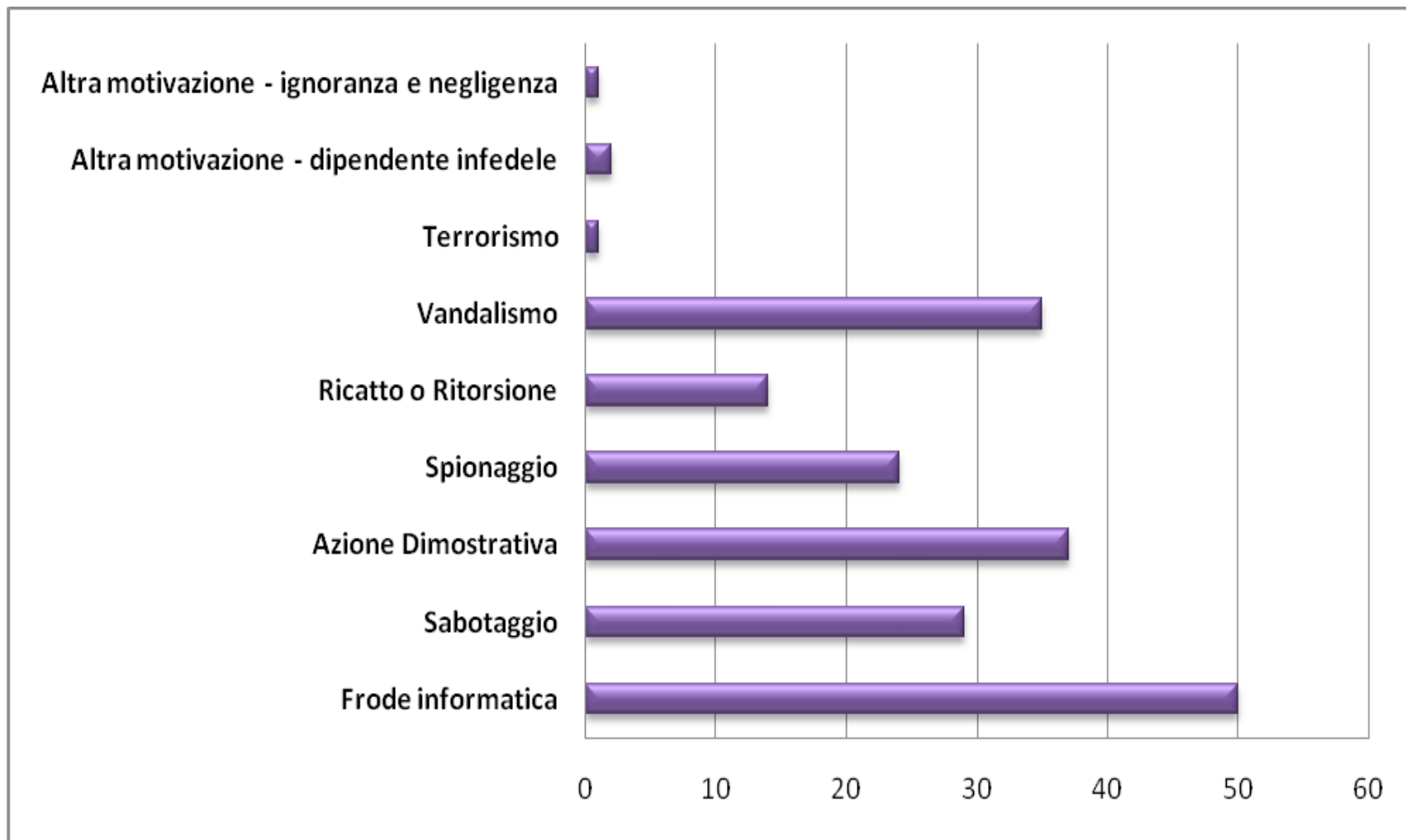
---

- i settori servizi (include Banche, Assicurazioni, Utilities, Distribuzione/Retail, Trasporti, Servizi Professionali, Sanità, Istituzioni Finanziarie non Bancarie, Istruzione & Ricerca) e ICT hanno un buon “bilanciamento” tra i diversi tipi di misure e strumenti;
- il settore industria (include l'industria manifatturiera e farmaceutica) è piuttosto carente sui vari strumenti di controllo, monitoraggio, IPS/IDS, e sui sistemi più avanzati di identificazione e autenticazione;
- le PA (Pubbliche Amministrazioni sia Centrali che Locali) non dispongono o dispongono in maniera ridotta di sistemi ad alta affidabilità, di strumenti di crittografia, di autenticazione forte degli utenti. È anche limitata la diffusione di policy della sicurezza e delle procedure organizzative.

# OAI 2009: % tipologia attacchi più temuti



# OAI 2009: Ripartizione percentuale delle motivazioni per i potenziali attacchi



# Indice

---

1. L'iniziativa OAI, Osservatorio Attacchi Informatici in Italia

1. Il Rapporto 2009

***1. I prossimi passi per il Rapporto 2010***

# I prossimi passi

---

- Si sta già impostando la raccolta on-line del prossimo Rapporto OAI 2010:
  - Migliorando il questionario
  - Coinvolgimento di altre Associazioni ed Istituzioni
  - Ampliamento e miglior bilanciamento del numero di rispondenti per settore
  - Copertura attacchi rilevati nell'intero arco del 2009 e nel primo trimestre 2010
- Si è costituito il Gruppo di Lavoro OAI con la partecipazione di esperti da parte degli attuali Patrocinatori, cui si è già aggiunto itSMF e nel prossimo futuro ulteriori enti quali Assinform ed Assintel.
- Il nuovo questionario on line su web per il 2010 sarà disponibile per la fine di **giugno – luglio 2010**
- Disponibilità Rapporto 2010 prevista entro fine **ottobre 2010**

# La continuità di OAI tra i Rapporti annuali

Da marzo 2010 sulla rivista **Office Automation** tengo una rubrica fissa mensile per OAI sugli attacchi informatici, con un taglio più manageriale che tecnico.



## Attacchi informatici: non si scherza più

Da questo numero prende il via una rubrica mensile sugli attacchi ai sistemi collegata all'OAI (Osservatorio Attacchi Informatici in Italia) voluto da Fi e dal ClubTI di Milano insieme a Soiel International, con il patrocinio di



## Non esiste sicurezza senza l'utente finale

Secondo appuntamento con la rubrica OAI (Osservatorio Attacchi Informatici). Il comportamento di utenti e operatori è determinante per la sicurezza aziendale. Nonostante i progressi tecnologici, se si sottovalutano aspetti di formazione e sensibilizzazione, i rischi continueranno a crescere.

