Insicurezza digitale sistemica: cosa emerge dal Rapporto OAD 2024

Webinar AIPSI-AICA 21/11/2024 ore 17

Marco R. A. Bozzetti
Presidente AIPSI (m.bozzetti@aipsi.org)
Founder e CEO Malabo srl (www.malaboadvisoring.it)

AIPSI, capitolo italiano della mondiale ISSA

- Associazione no-profit di **sole persone fisiche**
- Obiettivo principale: **l'indirizzamento e la crescita professionale dei suoi Soci**
- Tre tipologie di Socio;
  - AIPSI-ISSA (US$ 160,00 /anno)
  - SOLO AIPSI (€ 50,00/anno)
  - AIPSI GIOVANE (fino a 26 anni: primo anno gratuito, poi € 25,00/anno)
  - Si veda: https://www.aipsi.org/associazione/come-associarsi.html
- Socio FIDAInform

- **Servizi riservati a tutti i Soci AIPSI**
  - **supporto alle certificazioni**, in particolare per **eCF Plus** (EN 16234-1:2016) per profili sulla sicurezza digitale con **con forti sconti**
  - **Mentoriship gratuita sull'indirizzamento e sulla crescita professionale**
  - **SIG di approfondimento e discussione**:
    - AI e Cybersec
    - Crescita professionale Soci
  - ***Network Soci a livello nazionale***
- **Servizi riservati ai Soci AIPSI-ISSA**
  - **ISSA Journal**
  - **ESG ISSA Survey "The Life and Times of Cyber Security Professionals"**
  - Convegni, workshop, webinar in inglese
  - Corsi online in inglese
  - **SIG, Special Interest Group**
    - Privacy
    - Women in Security
  - **Accordi con sconti per certificazioni individuali**
  - ***Network Soci a livello mondiale***

L’indagine OAD/OAI dal 2007 ad oggi

- **17 anni consecutivi di indagini**
  - basate su questionari online anonimi
  - libero accesso al questionario per tutti i referenti di un sistema informativo operante in Italia
- **Per tutti i settori merceologici + Pubbliche Amministrazioni Centrali e Locali**
- **13 Rapporti pubblicati**
- Uno **specifico sito web** che costituisce il **repository** di tutti i Rapporti OAD/OAI pubblicati e della documentazione sui vari eventi e sugli articoli pubblicati nei quali AIPSI ha presentato dati emersi dalle indagini: www.oadweb.it

OAD è l'unica indagine online in Italia (completamente indipendente e “terza” rispetto ai vari attori in gioco) sugli attacchi digitali intenzionali ai sistemi informativi delle aziende e degli enti pubblici operanti in Italia, e sulle misure tecniche ed organizzative che questi hanno in esercizio. OAD non predefinisce uno specifico bacino di rispondenti, il medesimo negli anni, ma consente a chiunque, interessato e coinvolto nella gestione di un sistema informativo di una azienda/ente, un pieno e libero accesso al questionario online, in maniera totalmente anonima.

Il Rapporto OAD 2024 di AIPSI

- Il **Rapporto OAD 2024** è di 192 pagine A4, con 141 immagini e grafici.
- E' strutturato in 8 Capitoli (141 pagine A4) con l'elaborazione e l'analisi dei dati emersi dall'indagine e in 8 Allegati (49 pagine A4).
- **Prefazioni** di:
  - Ivano Gabrielli, **Direttore del Servizio Polizia Postale e per la Sicurezza Cibernetica**
  - Alessandro Musumeci, **Capo della Segreteria Tecnica del Sottosegretario all'Innovazione Tecnologica**
- Nel Capitolo 8 sono riportati i dati forniti e commentati dalla Polizia Postale e per la Sicurezza Cibernetica.
- Il Rapporto fornisce nei Capitoli 1 ed 1bis l'Executive Summary in italiano e in inglese.
- **Sponsor**: Qintesi Spa
- **Patrocinatori**: AICA, AIPSA, AISIS, Anasin-Assinform, ANIPA, ASSI-Bologna, Anorc, Aused, CIOClub Italia, Club Dirigenti Informatica (CDI), Club Dirigenti Tecnologie dell'Informazione (CDTI), Club Tecnologie dell'Informazione Emilia Romagna, ClubTI Liguria, ClubTI Milano, FIDA Inform, CSIG, INFORAV, SESAMO.

Rapporto OAD 2024 liberamente scaricabile da: https://www.aipsi.org/aree-tematiche/osservatorio-attacchi-digitali/oad-2024/rapporto-oad-2024-pubblicato-e-scaricabile.html

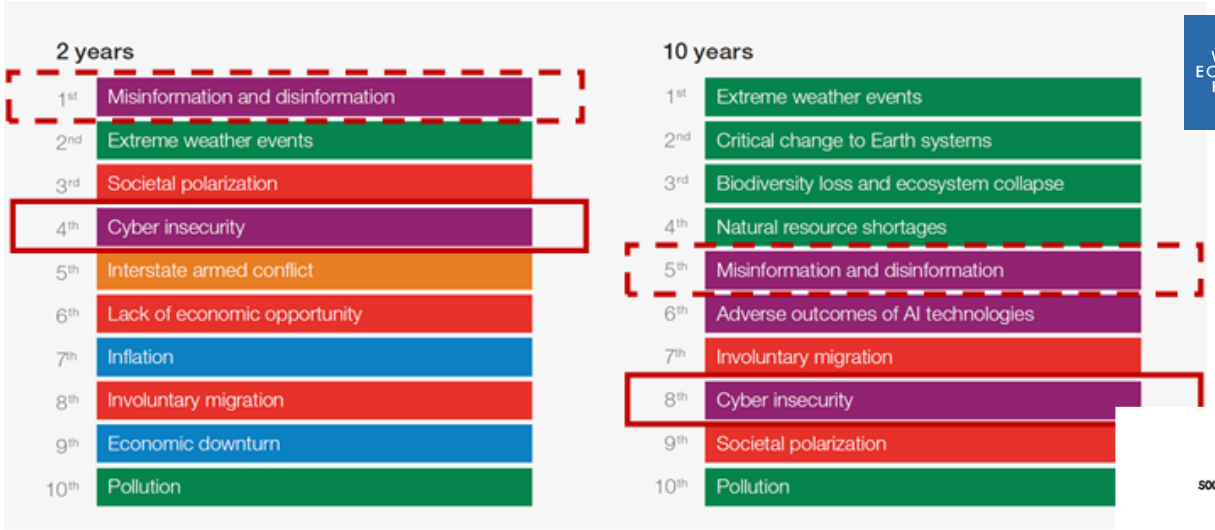
I contenuti del Rapporto OAD 2024

- Inquadramento attacchi e rischio informatico a **livello mondiale → WEF** (Cap. 3, Cap. 3.2))
- Inquadramento attacchi e rischio informatico a **livello europeo → ENISA** (Cap. 3.1)
- Inquadramento attacchi e rischio informatico a **livello italiano**:
  - **ACN** (Cap. 3.1)
  - **Servizio Polizia Postale e per la Sicurezza Cibernetica** (Cap. 3.1, Cap. 8)
- **Risultati dell'indagine OAD 2024** (Cap.4)
  - Attacchi digitali rilevati nel 2023
    - Più diffusi attacchi rilevati dai rispondenti
    - Approfondimento verticale per attacchi agli ambienti web
    - Approfondimento verticale per attacchi agli ambienti OT, Operational Technology
  - Misure di sicurezza digitale in atto: domande opzionali, compilate dal **35,4 %** di tutti i rispondenti

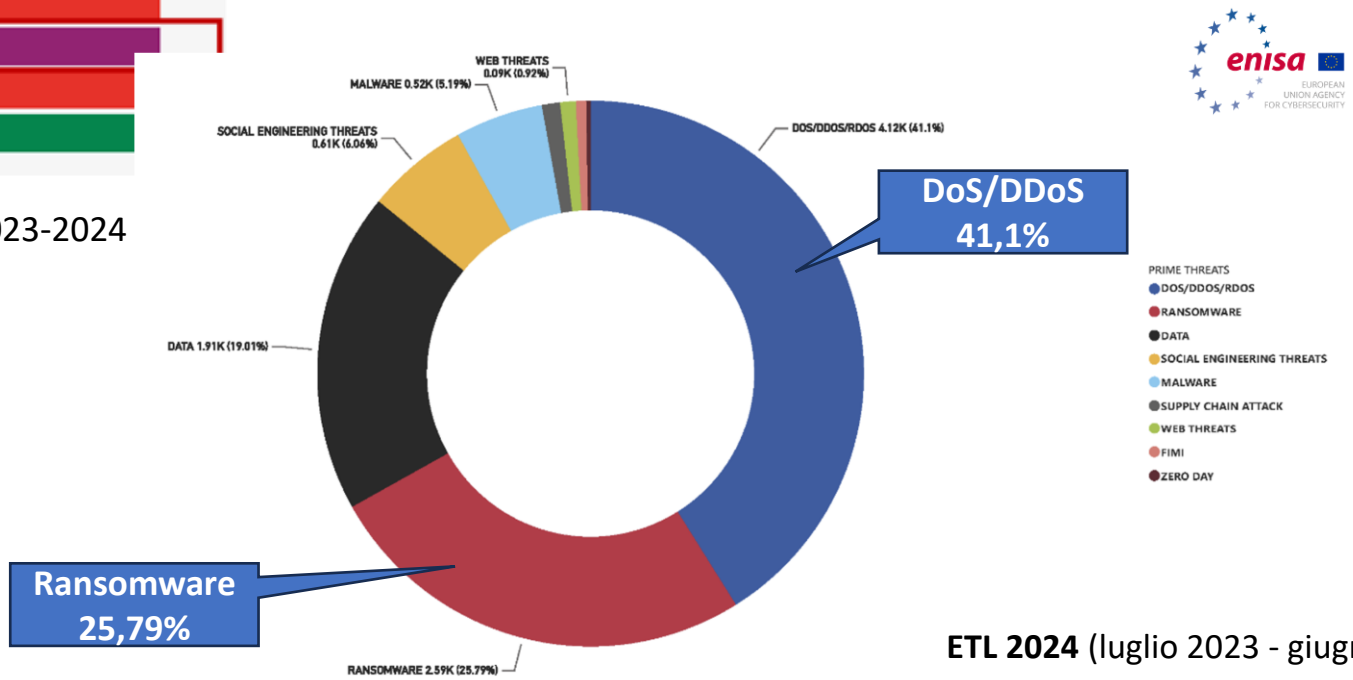
Tipologie e tecniche di attacco in OAD

- **Tipologie di attacco digitale**
  - ***Che cosa si attacca*** → *obiettivo attacco*
    - *Dal singolo dispositivo fisico alle reti e alle applicazioni*
    - *Considerate 14 tipologie → slide 11*
- **Tecniche di attacco digitale**
  - ***In che modo e con quali tecniche si attacca***
    - *Considerate 7 famiglie di tecniche → slide 11*

Il quadro degli attacchi/rischi digitali a livello mondiale ed europeo



World Economic Forum Global Risks Perception Survey 2023-2024



ETL 2024 (luglio 2023 - giugno 2024)

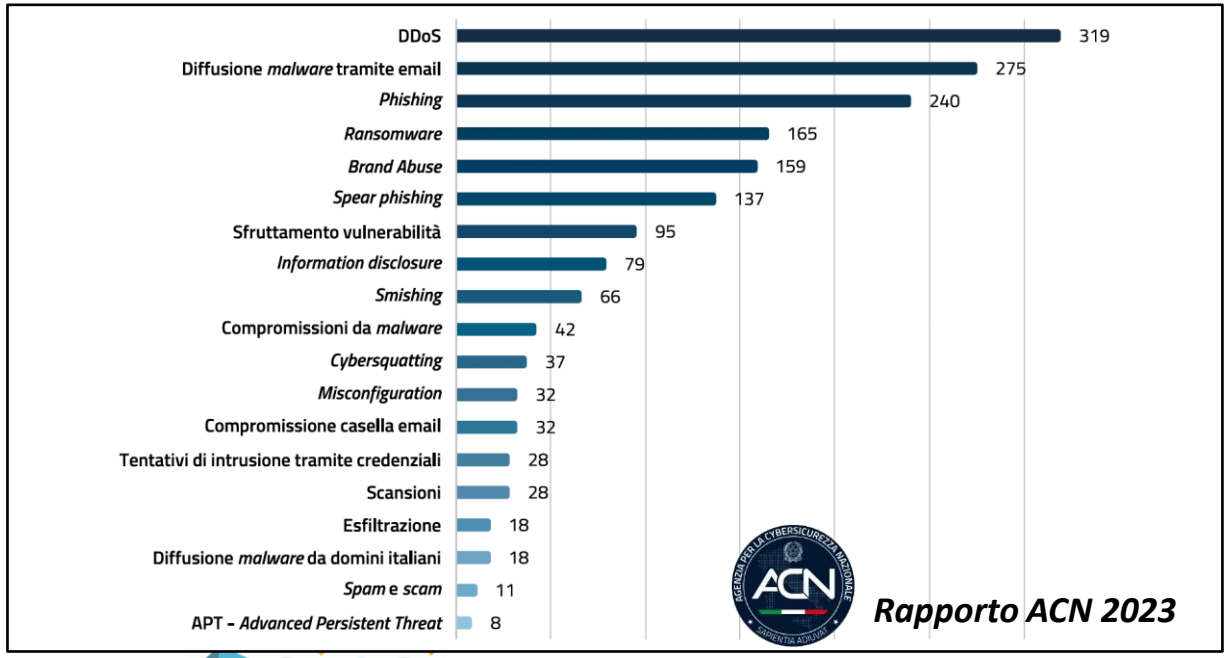
A livello italiano da Polizia Postale e ACN

Protezione strutture critiche/essenziali	1 gen - 30 giugno 2024	1 gen - 31 dic 2023	1 gen - 31 dic 2022	1 gen - 30 apr 2021	1 gen - 31 dic 2020	1 gen - 31 dic 2019	1 gen – 31 dic 2018	1 gen – 31 dic 2017	1 gen – 31 dic 2016
Attacchi rilevati (*)	5.903 **	12.101 **	13.099	282	509	1181	459	1.032	844
Alert diramati	31.033	77.012	113.420	24.824	83.416	82.484	80.777	31.524	6.721
Indagini avviate (***)	36	96	110	34	103	155	74	72	70
Persone denunciate/indagate (*)	101 **	224 **	334	n.d.	105	117	14	1.316	1.226
Richiesta di cooperazione internazionale in ambito Rete 24/7 High Tech Crime G8 (Convenzione Budapest)	23	79	77	17	69	79	108	83	85
Indagini avviate su attacchi rilevati	0,61%	0,79%	0,84%	12,06%	20,24%	13,12%	16,12%	6,98%	8,29%
Persone indagate su attacchi rilevati	1,71%	1,85%	2,55%	n.d.	20,63%	9,91%	3,05%	127,52%	145,26%

* Per il 2023-24: Target: Infrastrutture Critiche (I.C.), Operatori Servizi Essenziali (OSE), Pubbliche Amministrazioni Locali (PAL), Aziende, Privati

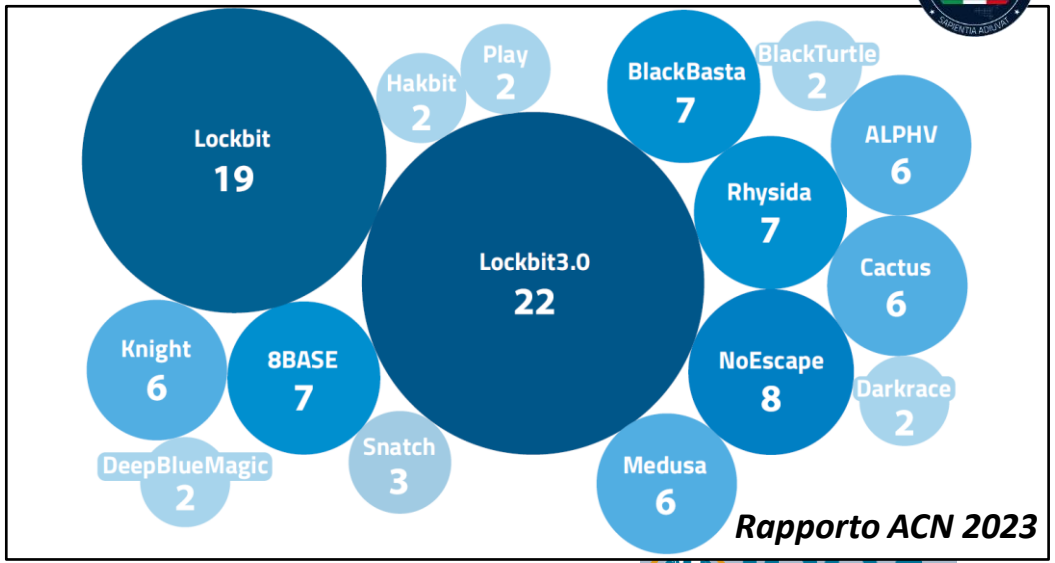
** Per il 2023-24: Dati aggregati C.N.A.I.P.I.C. e Centri Operativi per la Sicurezza Cibernetica (C.O.S.C.).

*** Per il 2023-24 dal C.N.A.I.P.I.C.



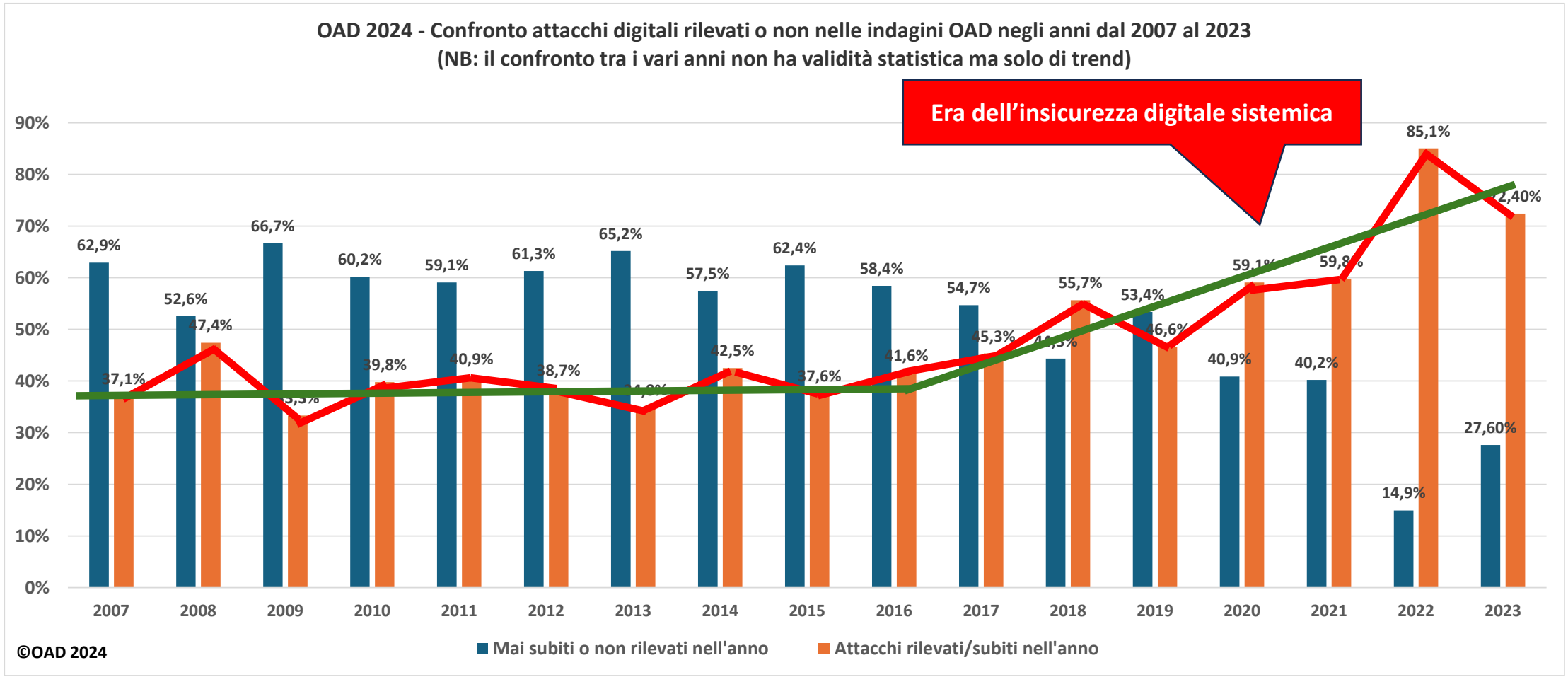
Rapporto ACN 2023

Diffusione gruppi hacker di ransomware

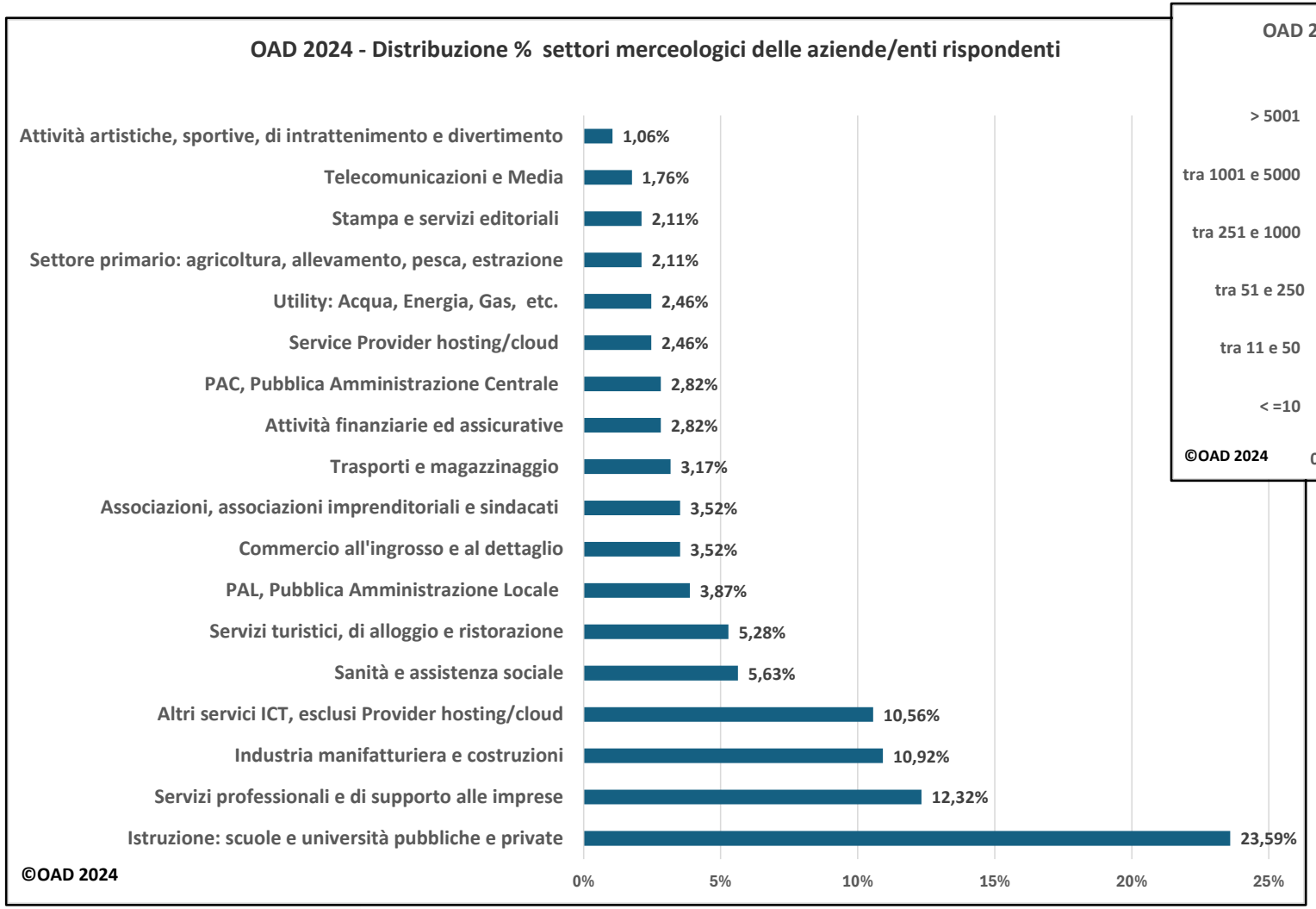


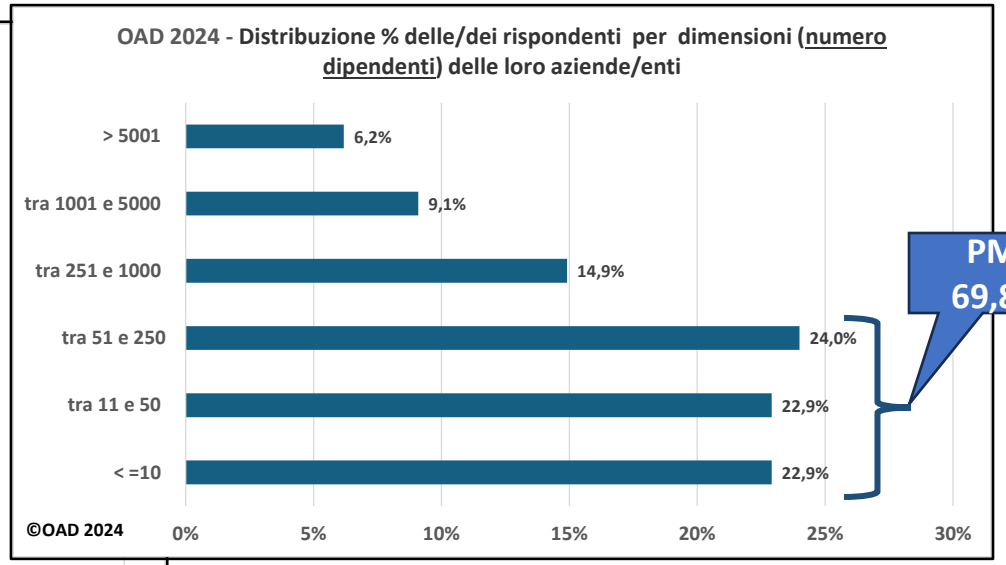
Rapporto ACN 2023

Il trend degli attacchi digitali dalle indagini OAD 2007-2023



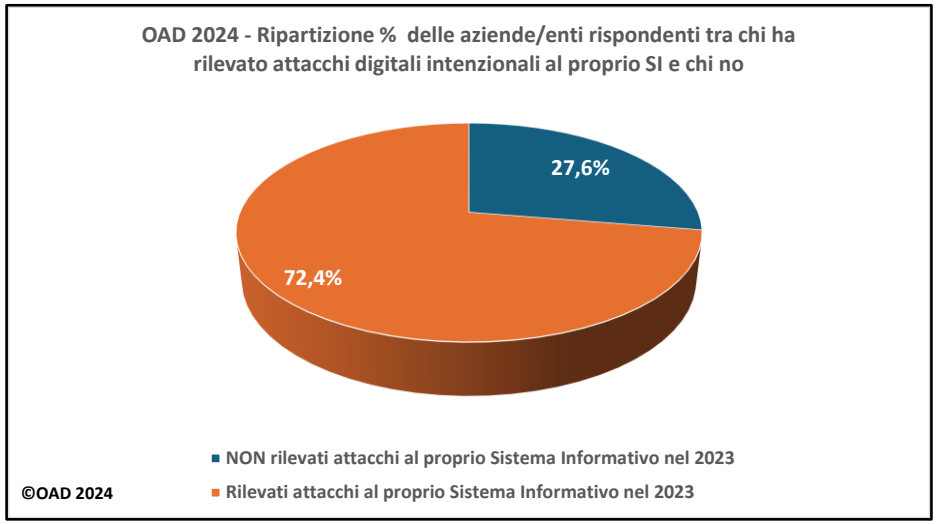
OAD 2024: Settore merceologico delle aziende/enti rispondenti

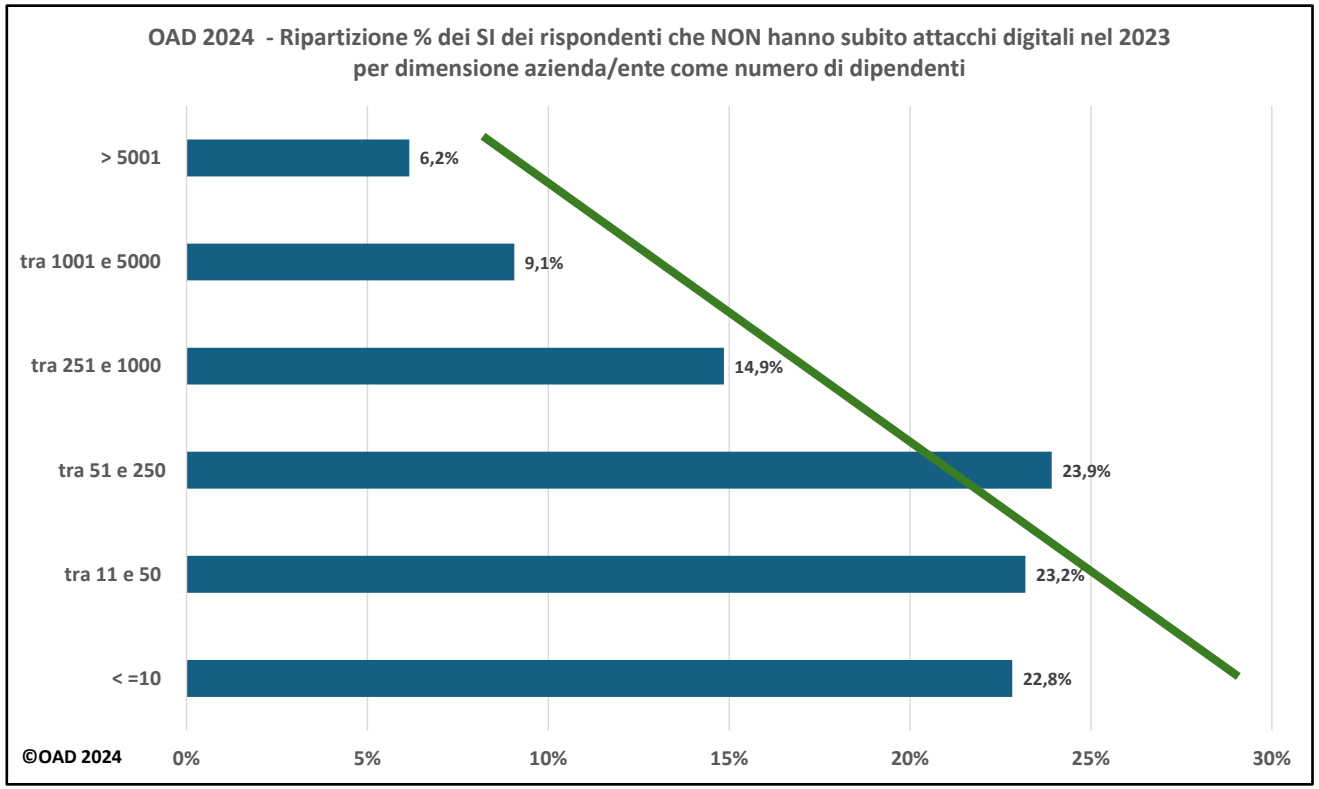




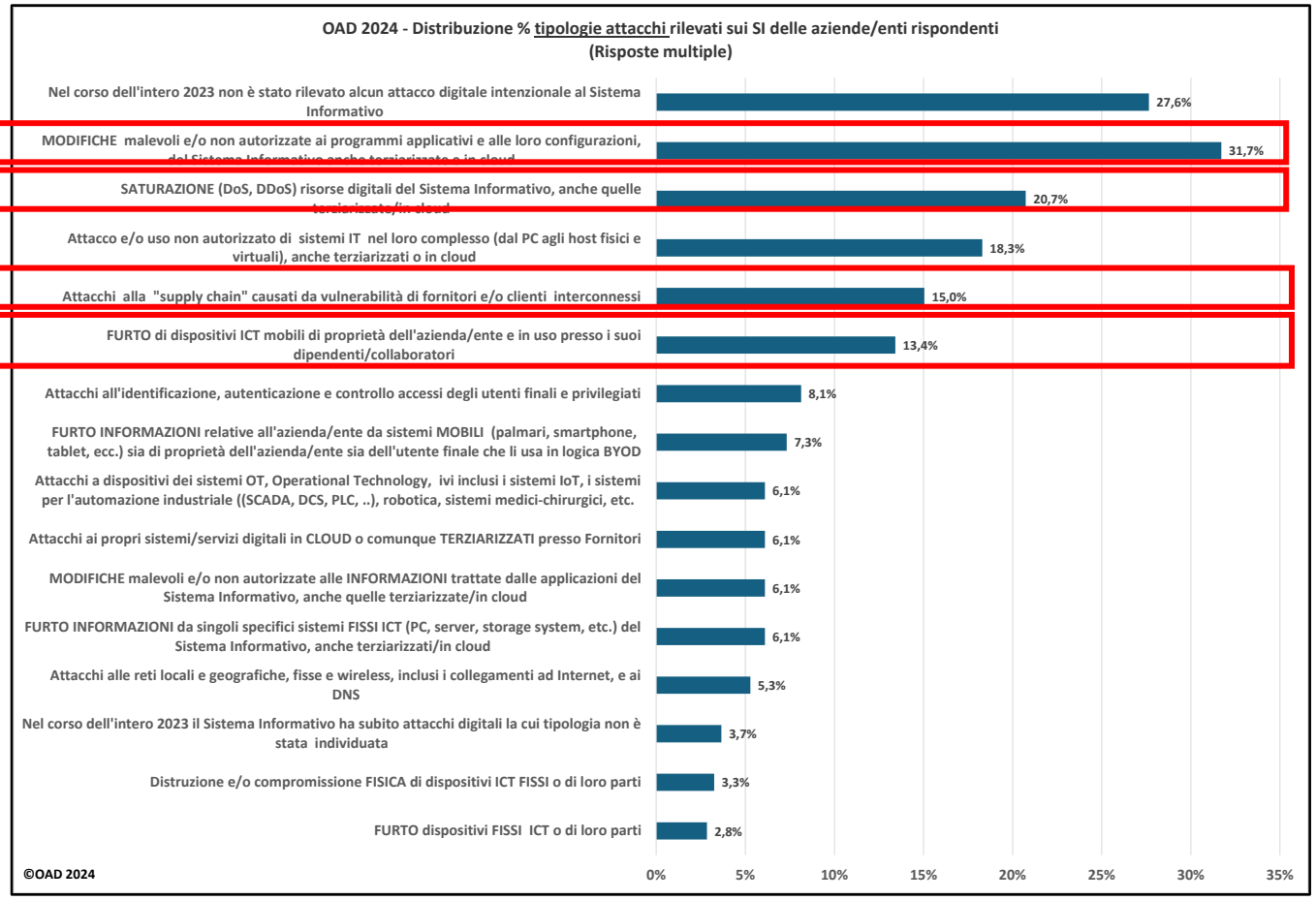
Numero addetti	Numero imprese	% aziende/classe addetti
0-9	4.427.716	94,9%
10-49	207.173	4,4%
50-249	26.126	0,6%
da 250 in su	4.408	0,1%
Totale	4.665.423	
Totale PMI	4.661.015	99,9%

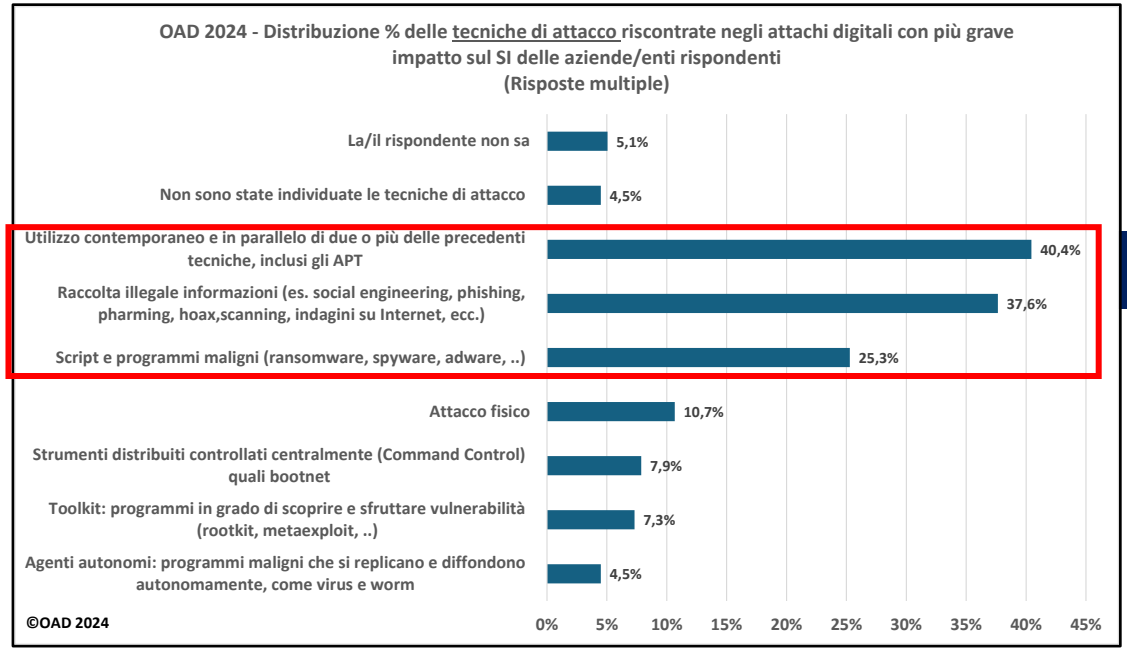
OAD 2024: attacchi digitali rilevati e correlati alla dimensione dell'azienda/ente rispondente (# addetti)



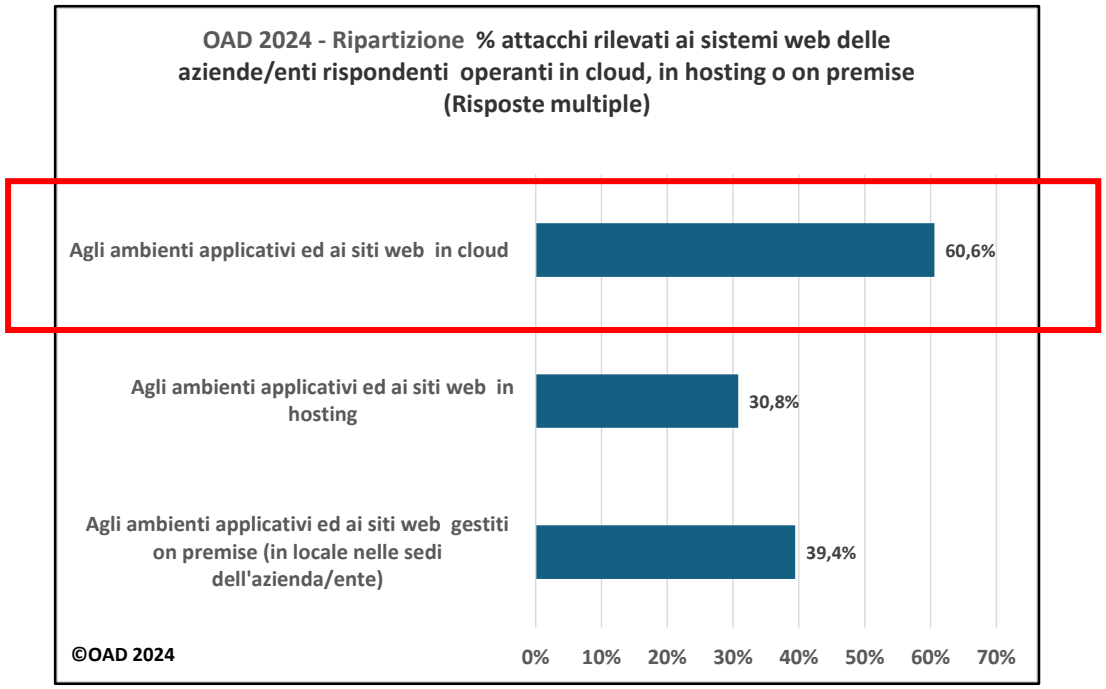


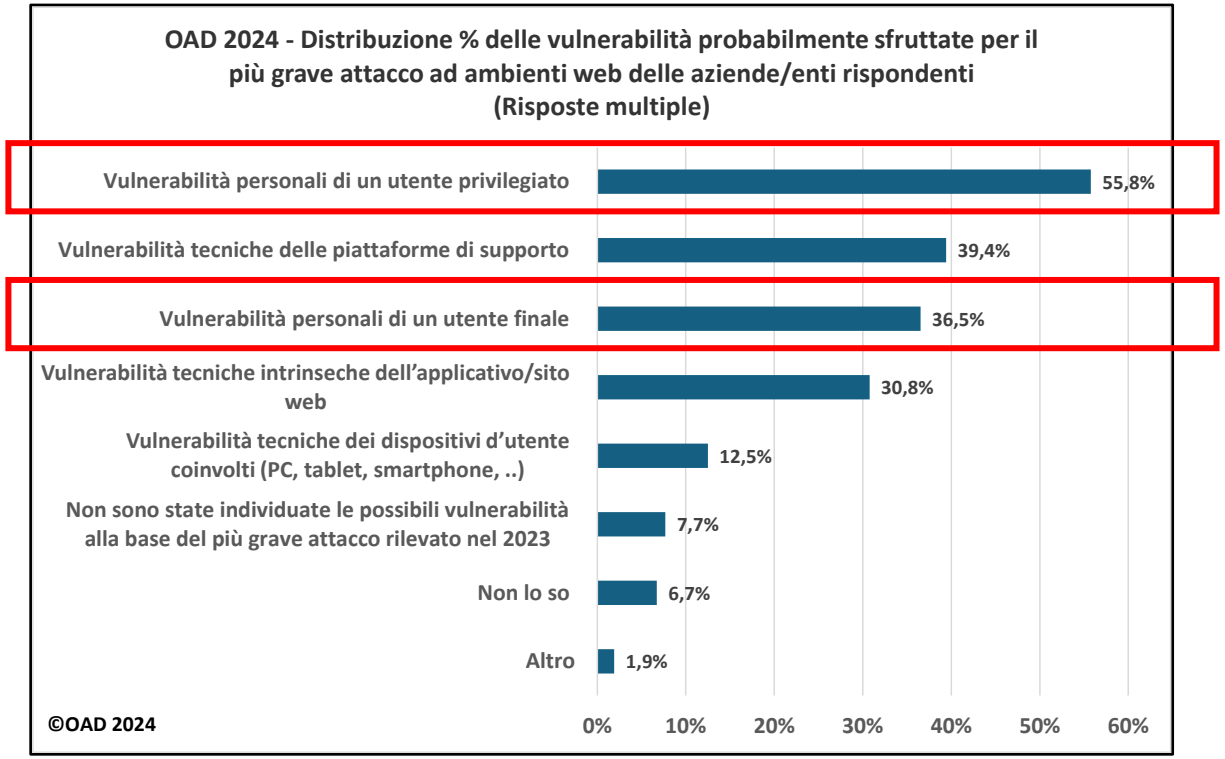
OAD 2024: Tipo e tecniche di attacco più diffuse



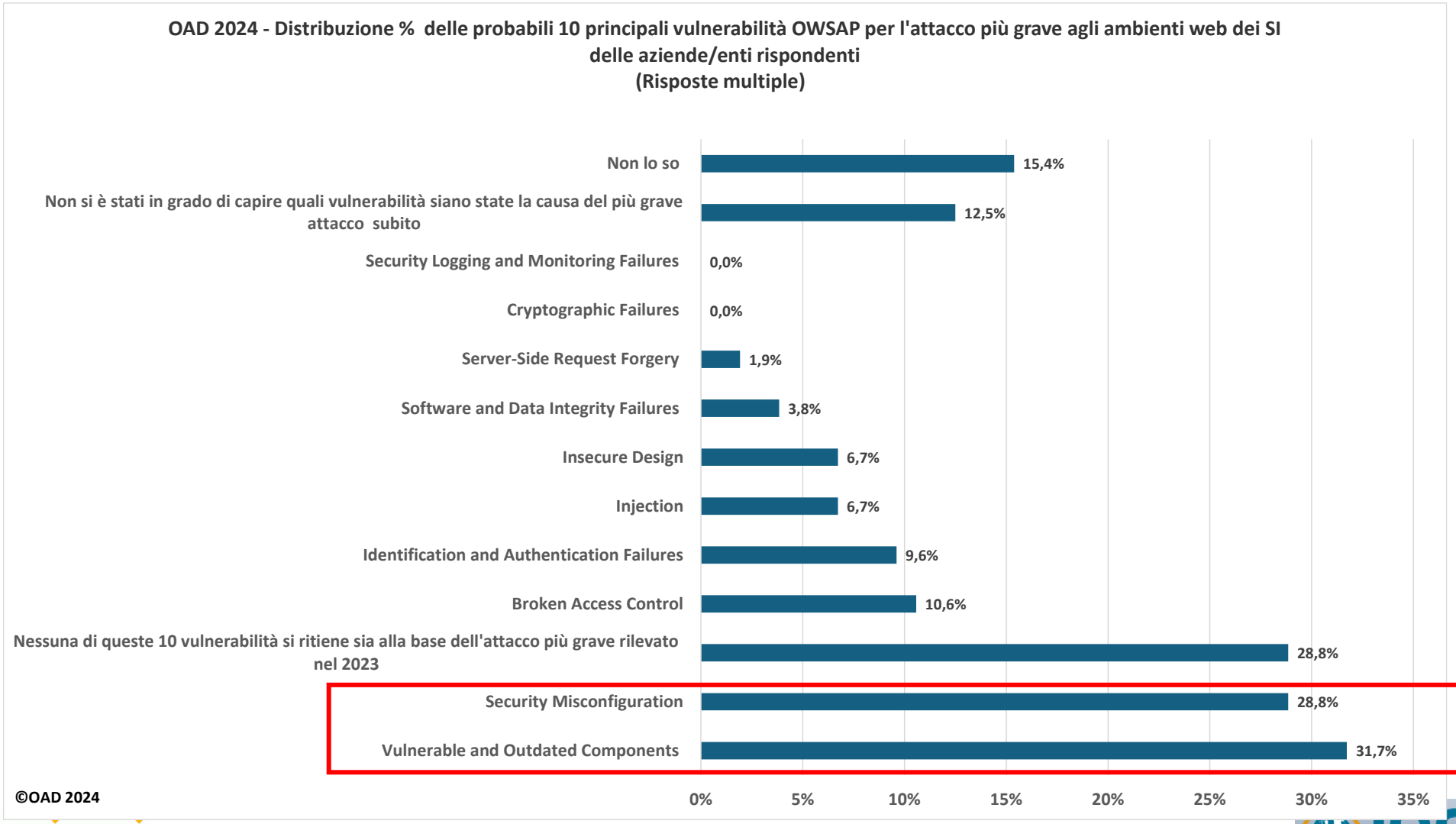


OAD 2024: attacchi agli ambienti web

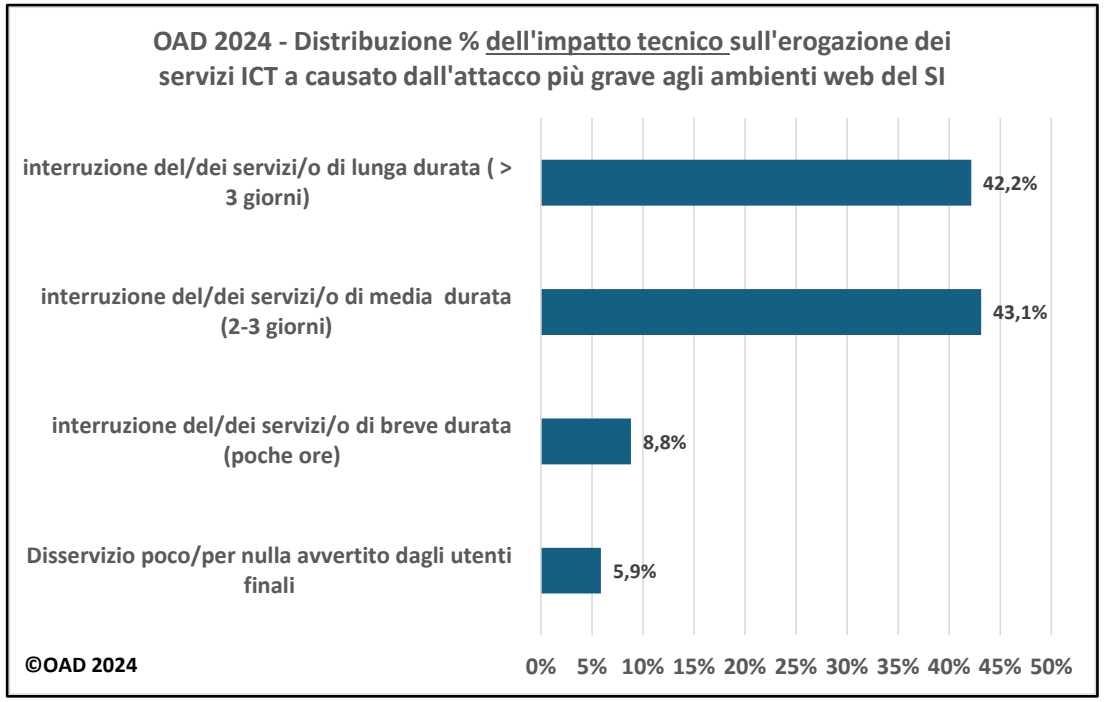


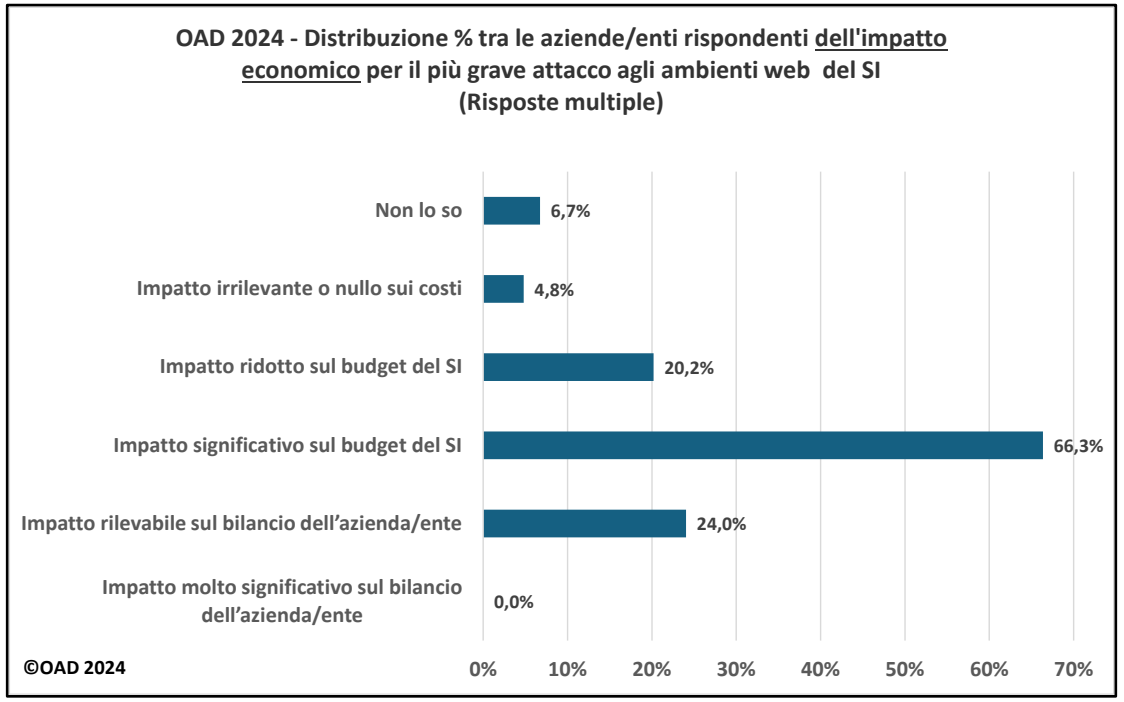


OAD 2024: principali rischi sfruttati (rif. Top Ten OWSAP)

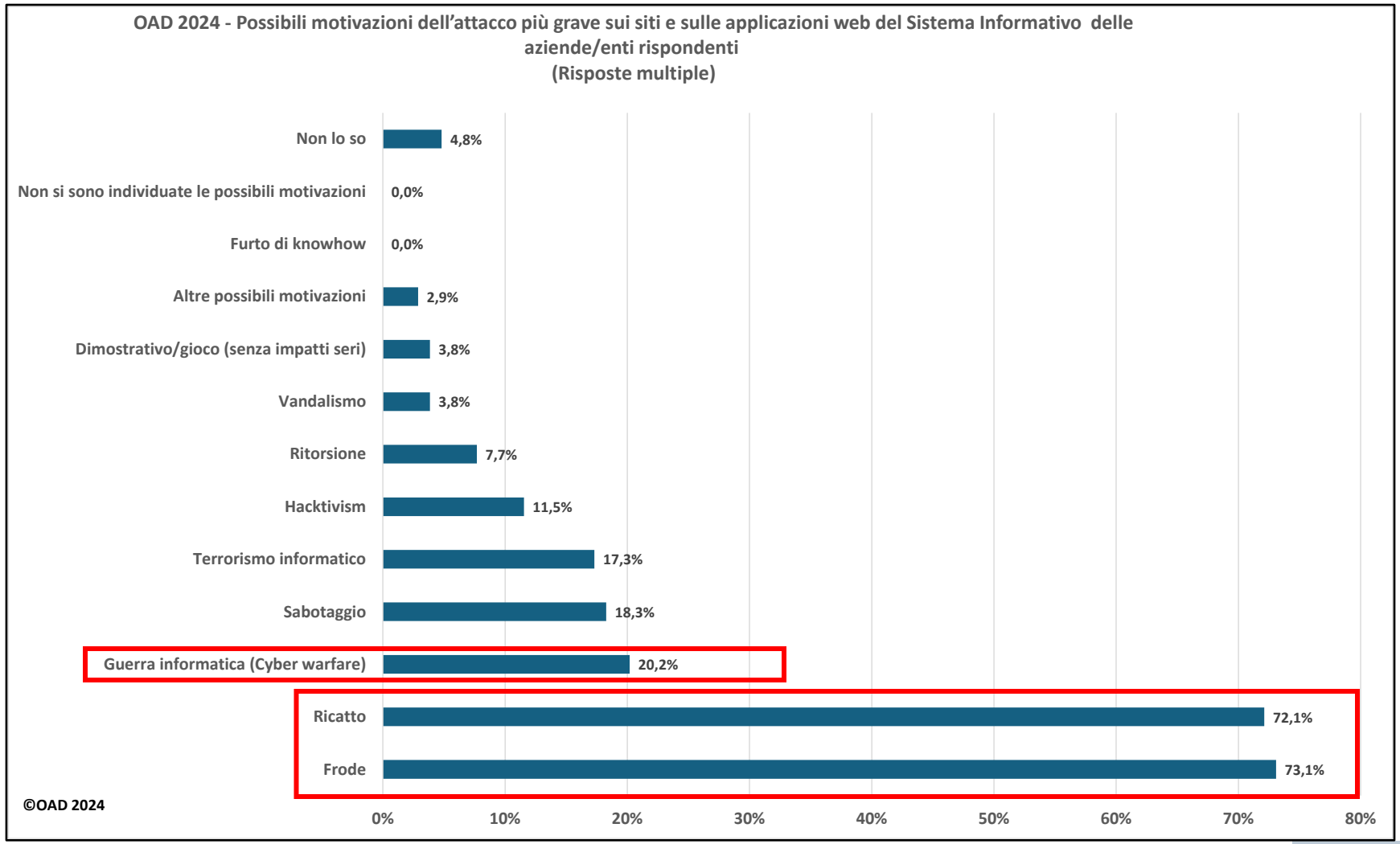


OAD 2024: gli impatti tecnici ed economici del più grave attacco agli ambiti web

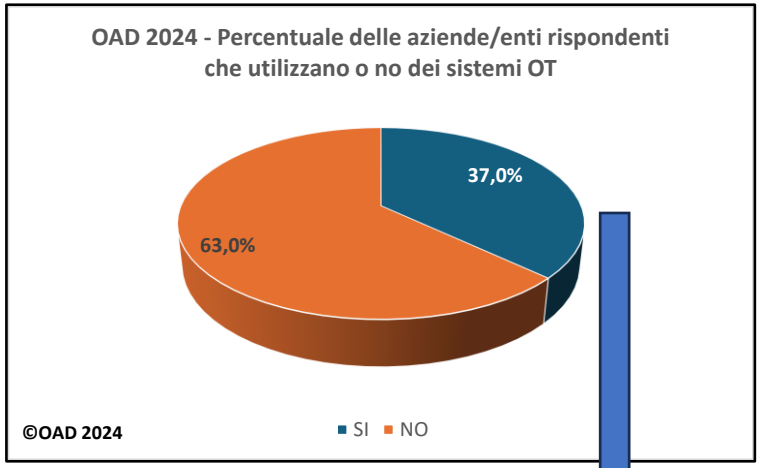


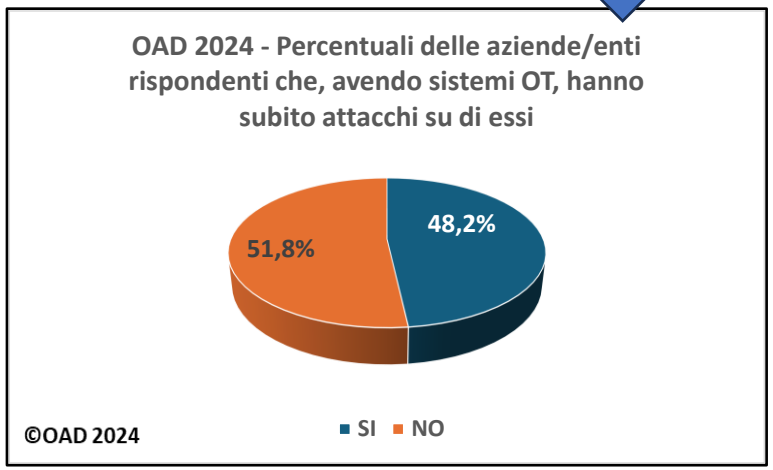


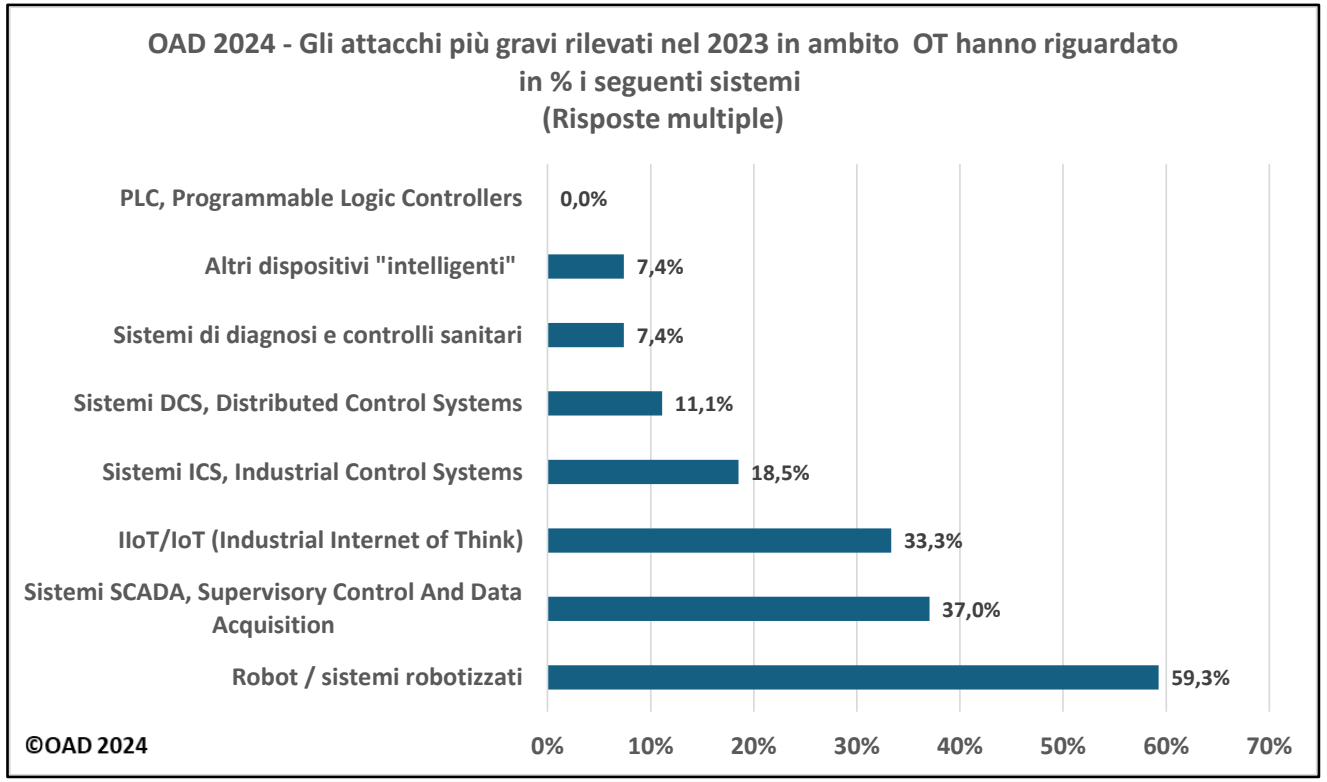
OAD 2024: le probabili motivazioni per il più grave attacco agli ambienti web



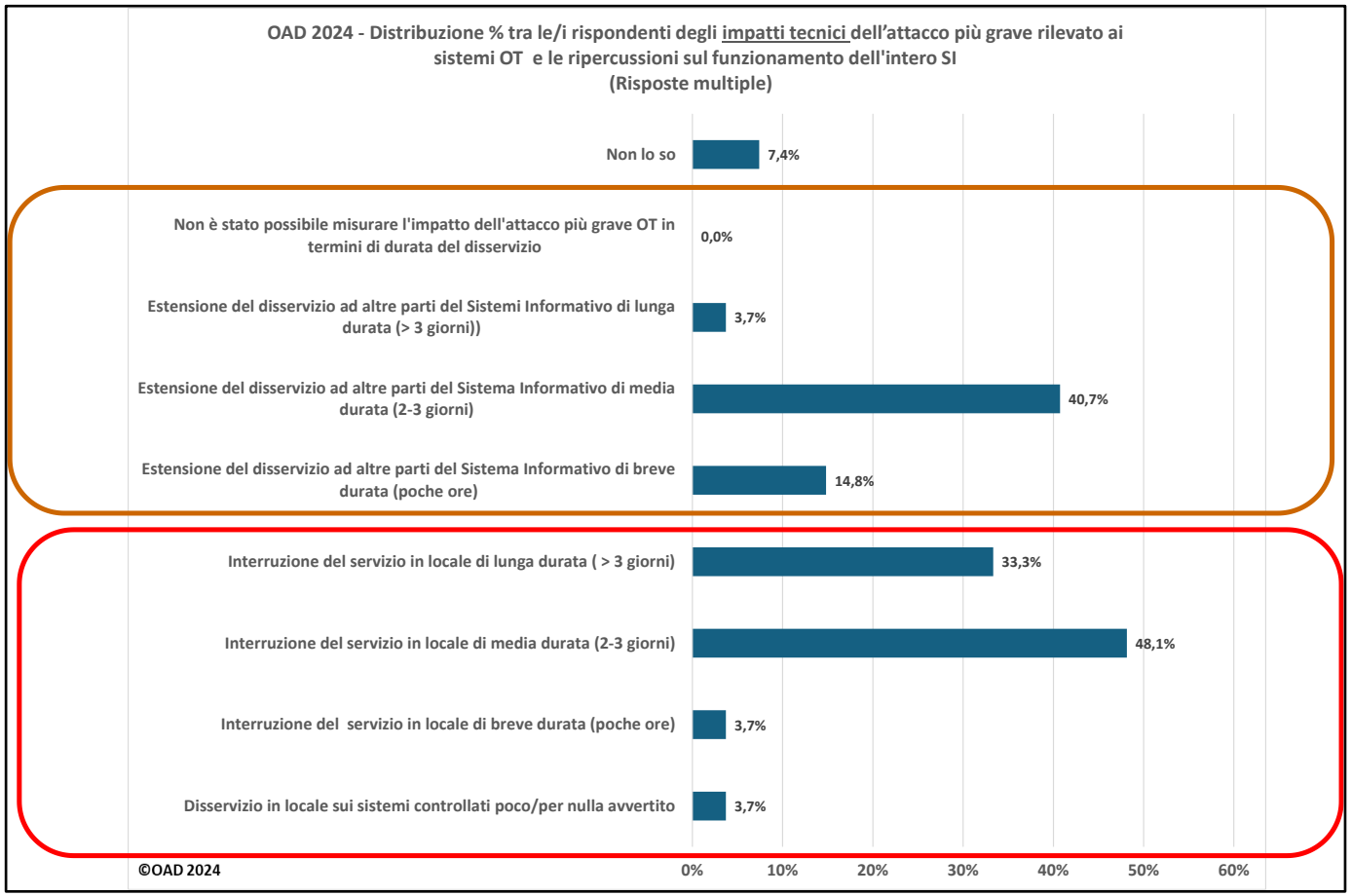
OAD 2024: attacchi agli ambienti OT, Operational Technology

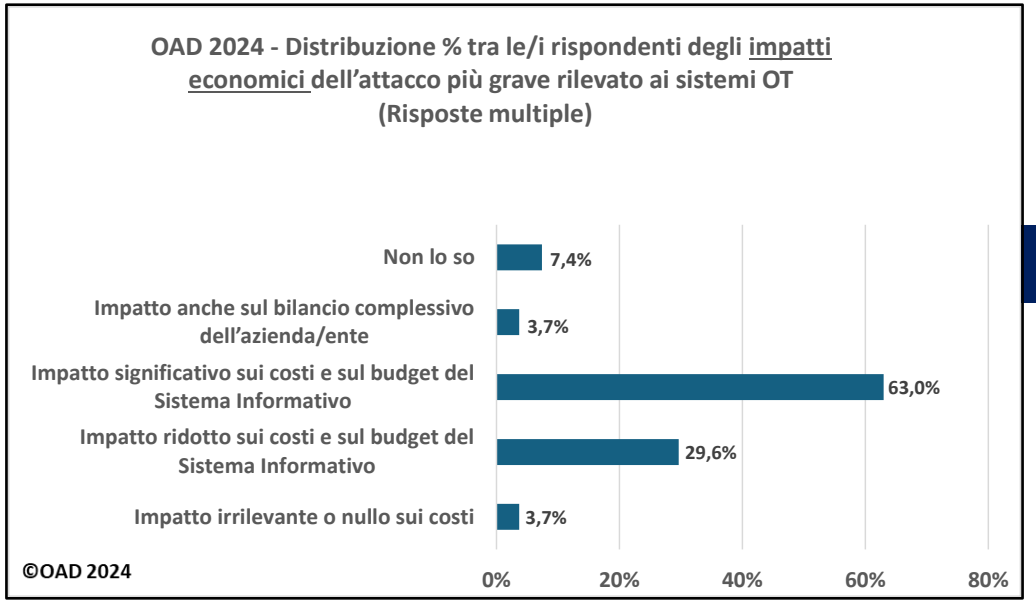




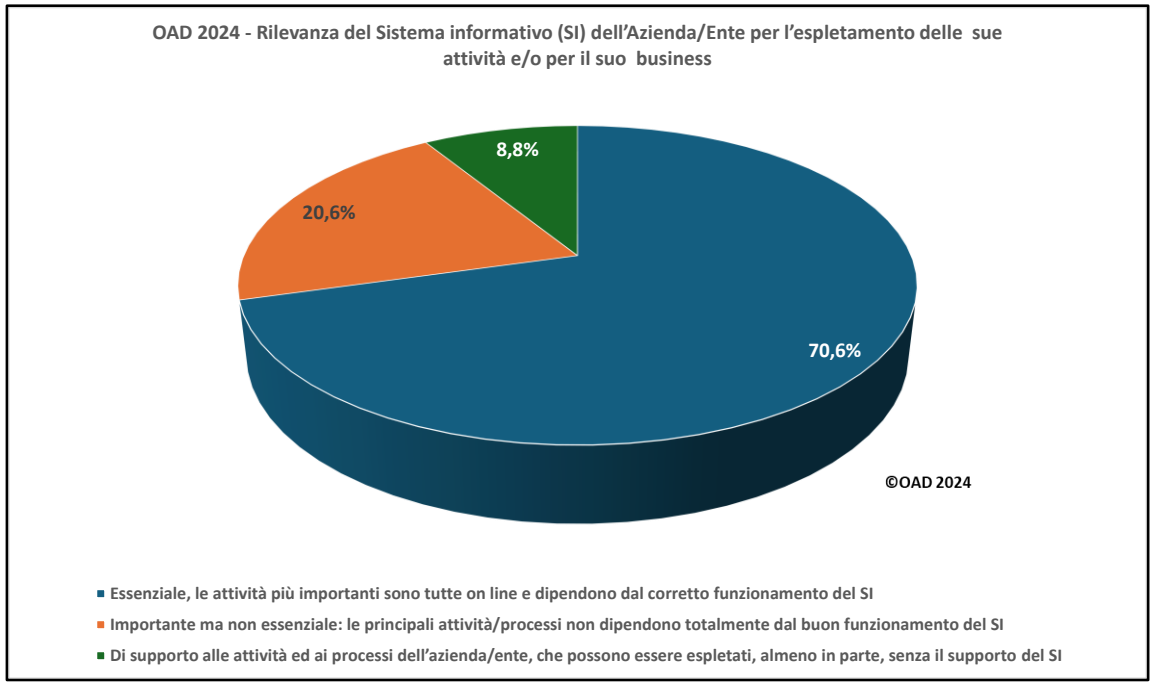


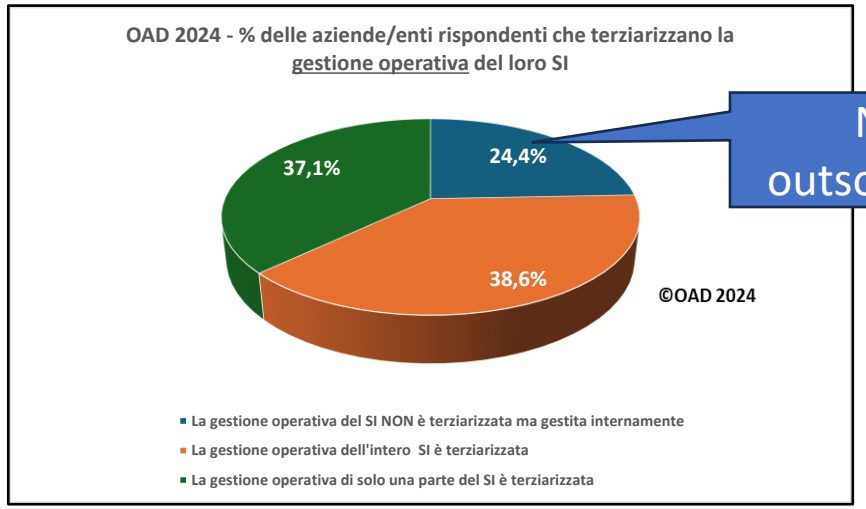
OAD 2024: gli impatti tecnici ed economici del più grave attacco agli ambiti OT

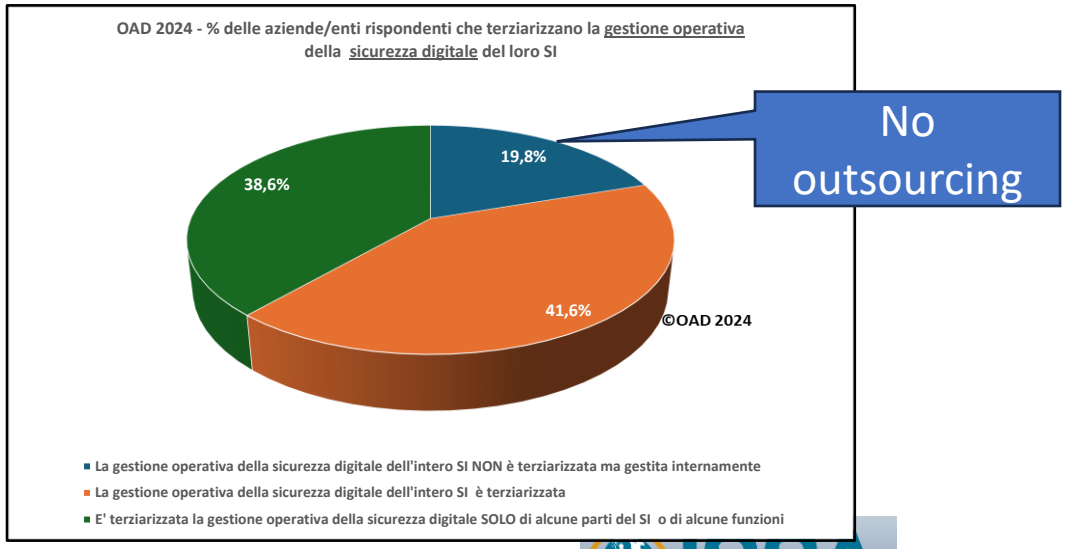




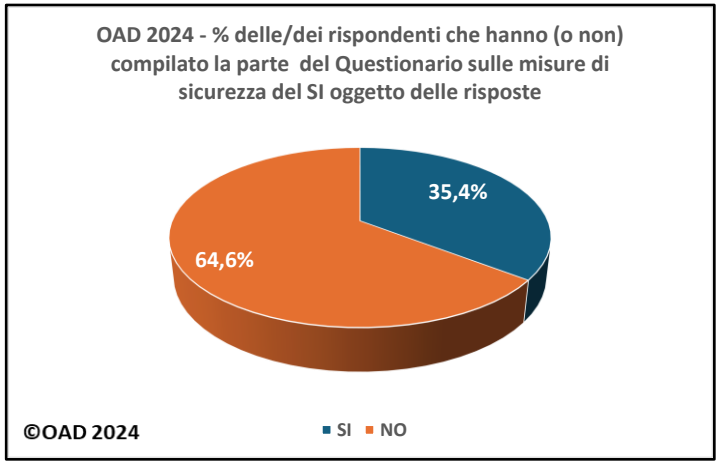
OAD 2024: importanza del SI ed uso di terziarizzazioni per la gestione del SI e della sua sicurezza digitale







OAD 2024: buon livello delle misure di sicurezza digitale in essere dichiarate



- **misure di gestione e controllo**
  - **l'80%** utilizza sistemi di gestione e di controllo in modalità diverse
  - Il **77,9%** archivia i log degli utenti, ed il **50%** li gestisce
  - Il **75%** ha previsto un **Piano di Disaster Recovery** (DR)
    - l'**83,3%** di queste ha previsto o allocato risorse ICT alternative per poterlo realmente attuare.

- **Misure organizzative** di sicurezza digitale
  - l'**81,3%** ha definito ed usa policy e procedure organizzative per la sicurezza digitale;
  - il **73,1%** ha policy e procedure per la gestione degli incidenti informatici
  - il **73,4%** effettua l'analisi dei rischi digitali;
  - il **60,9%** effettua auditing per la sicurezza digitale

- **Misure tecniche**
  - Il **60%** dispone di un Data Center in Italia con un elevato livello di affidabilità;
  - nell'**80%** dei casi sono previste misure per il controllo dell'**accesso fisico di persone** nei locali con sistemi ICT
  - il **54,3%** gestisce **centralmente le password**;
  - **71,6%,** dei SI **controlla centralmente** funzionalità, prestazioni e livelli di sicurezza delle reti;
  - il **33,3%** dei software applicativi sviluppati ad hoc hanno seguito procedure e metodiche di **sviluppo sicuro;**
  - **l'80%** dei SI usa **FWA**, **Firewall Applicativi;**
  - l'**84,7%** gestisce la **manutenzione correttiva** degli applicativi;
  - Il **78,5%** delle aziende/enti rispondenti effettua l'analisi delle vulnerabilità
  - il **44,6%** dei SI effettua il **backup** "a regola d'arte";
  - il **75,4%** ha e utilizza **procedure per il ripristino dei sistemi ICT dai dati di backup**

L’incontenibile INSICUREZZA digitale SISTEMICA …

- I dati emersi da OAD 2024 trovano sostanziale conferma nelle indagini e nei rapporti degli Enti istituzionali e di quelli privati/commerciali
- **Continua a permanere l’ampia diffusione di gravi attacchi digitali e di un forte rischio cibernetico a livello mondiale, europeo e in Italia**
- Nonostante gli investimenti spesso onerosi in misure di sicurezza, queste non sono riuscite, né riescono tuttora, a prevenire completamente gli attacchi informatici.
- Di fronte a questa situazione, le soluzioni attuali, che **richiedono un potenziamento anziché un abbandono**, devono essere **integrate** con politiche di **resilienza** per l'intera organizzazione ed il suo Sistema Informativo.
- **La resilienza** può e deve essere assicurata dalla **business continuity**, ossia la **continuità operativa dei processi essenziali**; mentre, sul versante ICT, da un piano di **Disaster Recovery** efficace, attuabile e testato.