Per una cybersecurity reale ed efficace: la situazione in Italia e considerazioni su come realizzarla e gestirla

Marco R. A. Bozzetti

- Presidente AIPSI (www.aipsi.org)
- CEO Malabo Srl (www.malaboadvisoring.it)
- Ideatore e curatore indagine OAD (www.oadweb.it)

OAD Osservatorio Attacchi Digitali in Italia

malabo ICT Advisory

Marco R. A. Bozzetti e Malabo Srl (www.malaboadvisoring.it)

malabo ICT Advisory

- Presidente AIPSI e CEO Malabo Srl, società di consulenza direzionale sull'ICT
- Ha operato con responsabilità crescenti presso primarie imprese di produzione, quali Olivetti ed Italtel, e di consulenza, quali Arthur Andersen Management Consultant e Gea/Gealab, oltre ad essere stato il primo responsabile dei sistemi informativi (CIO) dell'intero Gruppo ENI (1995-2000).
- Nella seconda metà degli anni 70 è stato uno dei primi ricercatori a livello mondiale ad occuparsi di internetworking, partecipando alla standardizzazione dei protocolli del modello OSI dell'ISO
- È certificato ITIL v3 ed EUCIP Professional Certificate "Security Adviser"
- Commissario d'Esame per le certificazioni eCF (EN 16234 - UNI 11506)
- Ha pubblicato articoli e libri sull'evoluzione tecnologica, la sicurezza digitale, gli scenari e gli impatti dell'ICT.

- Malabo Srl è stata creata da M. Bozzetti nel 2001
- una società di consulenza direzionale per l'ICT, che opera per Clienti lato domanda e lato offerta basandosi su una consolidata rete di esperti e di società ultra specializzate
- Obiettivo primario degli interventi di Malabo è di creare valore misurabile per il Cliente, bilanciando adeguatamente gli aspetti tecnici con quelli organizzativi nello specifico contesto del Cliente
- Dispone di un proprio laboratorio ICT con server e storage duali, virtualizzati, collegati con switch a 10 G e connessi ad internet con fibra ottica a 100 Mbps, oltre ad uno spazio in cloud (IaaS)
- Per garantire un effettivo trasferimento di know-how, fornisce come servizio ai Clienti le proprie metodologie e gli strumenti informatici usati nell'intervento consulenziale

AIPSI, Associazione Italiana Professionisti Sicurezza Informatica

- Associazione di **persone** apolitica e senza fini di lucro, **Capitolo Italiano** di **ISSA**, Information Systems Security Association, (www.issa.org) che conta + 12.000 Soci, la più grande associazione no-profit di professionisti della Sicurezza ICT nel mondo. Il Socio AIPSI è contemporaneamente Socio ISSA

- **Obiettivo principale**: aiutare i propri Soci nella **crescita professionale** → competenze →carriera e crescita business, offrendo ai propri Soci **servizi qualificati** per tale crescita, che includono
  - **Mentorship** ai Soci con un concreto supporto nell'intero ciclo di vita professionale, che può includere formazione specializzata e supporto alle certificazioni
    - **CSCL**, Cyber Security Career Lifecycle (ISSA)
    - **eCF Plus** (EN 16234-1:2016) per profili sulla sicurezza digitale
  - Rete professionale interpersonale tra i Soci AIPSI a livello nazionale e quelli ISSA a livello internazionale
  - Possibilità di nomine professionali come ISSA Senior Member, ISSA Fellow, ISSA Distinguished Fellow e ISSA International Awards
  - **Progetto AIPSI Giovani**
  - Gruppo di Lavoro **CSWI, Cyber Security Women Italy** , aperto a tutte le donne che in Italia operano a qualsiasi livello nell'ambito della sicurezza digitale (anche non socie AIPSI) Convegni, workshop, webinar sia a livello nazionale che internazionale via ISSA
  - **ISSA Journal** mensile
  - Rapporti annuali e specifici; esempi:
    - Rapporto annuale **OAD** nel sito **https://www.oadweb.it**
      - **Progetto OAD Extended 2021,** incluso tra le iniziative **di Repubblica Digitale**
    - **Rapporto** annuale indagine AIPSI **CSWI** sul lavoro femminali per la cybersec in Italia → **nuova indagine 2021 appena partita https://www.aipsi.org/breaking-news/753-parte-la-nuova-indagine-cswi-2021-sul-lavoro-femminile-nella-cybersecurity-in-italia.html**
    - ESG ISSA Survey "The Life and Times of Cyber Security Professionals"
  - Collaborazione con varie Associazioni ed Enti per eventi ed iniziative congiunte

Indagine OAD 2020 (www.oadweb.it)

- **OAD, Osservatorio Attacchi Digitali in Italia**: 12 anni consecutivi di indagini sugli **attacchi** intenzionali e le **misure di sicurezza** digitale di Aziende/Enti in Italia **Rapporto 2020 OAD completo**
  - **Costituito da 186 pagine A4, 148 immagini e grafici, 11 Capitoli (147 pagine A4) e 9 Allegati (39 pagine A4)**
  - **Nel Capitolo 11 i dati dalla Polizia Postale e delle Telecomunicazioni, commentati dall'autore**
  - **Executive Summary in italiano e in inglese**
- **Sintesi Rapporto 2020 OAD, 20 pagine A4**
- Gold Sponsor: **Cloudflare, Darktrace, Qintesi, Sophos**
- Silver Sponsor: Technology Estate
- Patrocinatori: AICA, AIPSI, AISIS, AITASIT, Anorc, Assi-BO, Assintel, Assolombarda, Aused, CDI Torino, CDTI Roma, Centro Ricerca sulla Scrittura, CIOClub, ClubTI Centro, ClubTI Emilia Romagna, ClubTILiguria, ClubTI Milano, FIDA Inform, Grafobiometristi Italiani Associati, IEEE-Italian Chapter, Inforav.

- **Rilevazione degli attacchi rilevati, delle loro caratteristiche, delle loro provabili motivazioni, dei loro impatti**
- **Rilevazione della macro caratteristiche del Sistema Informatico e delle misure di sicurezza tecniche ed organizzative implementate**
- **Macro caratteristiche dell'azienda/ente**

Indagine OAD 2020:
- **Intero 2019**
- **1° quarter 2020**

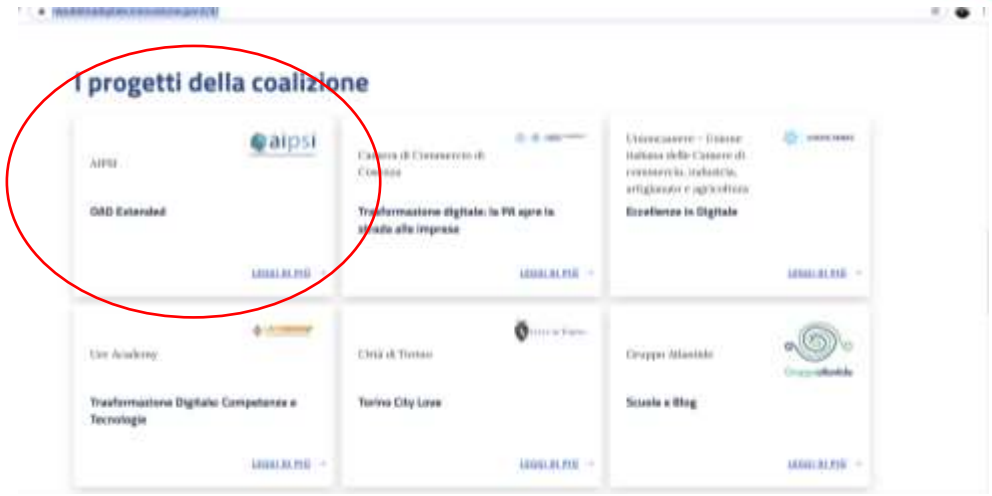
Entrambi scaricabili gratuitamente, dopo il login, da: https://www.oadweb.it/it/oad-2020/per-scaricaricare-la-sintesi-del-rapporto-2020-oad.html

Progetto AIPSI OAD Extended

https://repubblicadigitale.innovazione.gov.it/it/

@innovazionegov

#RepubblicaDigitale



OAD Extended: AIPSI chiede fin dal 2021 una effettiva collaborazione con Associazioni anche di categoria per estendere il numero di rispondenti, e per meglio motivarli, oltre che di lettori del Rapporto

- **OAD *Extended-PO*** : estendere il bacino di rispondenti/interessati ai vari settori merceologici + PA
- **OAD *Extended-SO*** : tre livelli nuovo questionario, tutti che forniscono una macrovalutazione integrabili tra loro per la produzione del Rapporto finale, basati su un sistema automatizzato/bile: 1) livello **base anonimo**, semplificato e ridotto nelle domande soprattutto sulle misure di sicurezza in essere; 2) livello **medio anonimo**, sile all'attuale ma con risposte semplificate e più chiare (per la macro valutazione) 3) livello **sofisticato non anonimo**, in grado di fornire specifiche informazioni di ausilio nell'assessment del livello di sicurezza del sistema informatico considerato e degli interventi opportuni per migliorarlo

La proposta di collaborazione per le Associazioni in https://www.aipsi.org/aree-tematiche/osservatorio-attacchi-digitali/oad-extended.html

La situazione attuale in Italia della cybersecurity con la pandemia Covid 19

La tipica situazione italiana di imprese private ed enti pubblici rispetto ai rispondenti OAD 2020

- **Aziende italiane** (dati Istat vs rispondenti OAD 2020): totale **4.404.501**
  - PMI: **99,91%** → OAD 2020 **57,7%**
  - Al di sotto di 10 dipendenti: 95% → **22,1%**

OAD 2020: buon bilanciamento e buona rappresentatività di aziende/enti per dimenioni (# dipendenti)

- **Pubbliche Amministrazioni (PA)**
  - Non si hanno dati certi sul numero complessivo di PA, si stima attorno ai 55.000, prevalentemente su PAL , PA Locali, ed anch'esse in stragrande maggioranza con pochi/pochissimi dipendenti
    - OAD 2020: PAC **2,9%**
    - OAD 2020: PAL **4,8%**

OAD 2020: partecipazione ridotta di alcuni settori merceologici
- **30% circa dei rispondenti del settore ICT**
- **Impossibilità di effettuare valide analisi per settore**
- **necessità del Progetto OAD Extended , partendo dall'indagine 2021**

L'effetto pandemia Covid 19 sulla cybersecurity in Italia

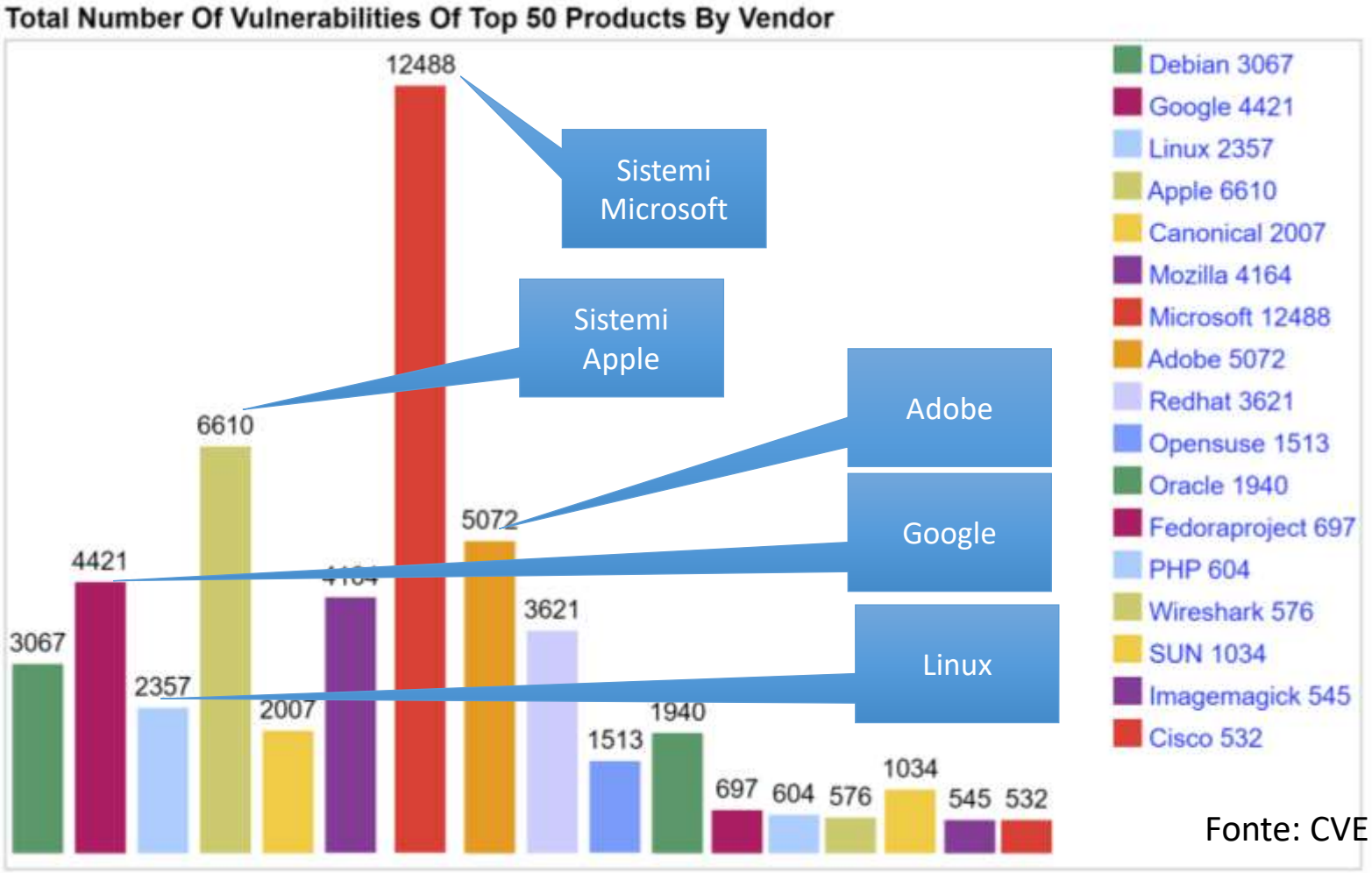
- Forte spinta alla digitalizzazione
- Rapido e largo uso di lavoro da remoto (agile/smart working) e di servizi via Internet (e-commerce, e-banking)
- Crescita nell'uso di soluzioni cloud anche per le applicazioni core business
- Maggior supporto richiesto alle infrastrutture ICT
- Crescita della necessità e in parte degli interventi per cybersecurity e per la resilienza anche organizzativa dell'azienda/ente
- Incremento di nuovi attacchi digitali (siti malevoli, malware, ransomware, tutti con riferimento al Covid), risultati efficaci soprattutto sulle piccolissime strutture, sovente non dotate di idonee e sufficienti misure di sicurezza digitale

Qualsiasi attacco digitale si basa su vulnerabilità

Vulnerabilità: carenza o debolezza di un sistema o di un essere vivente

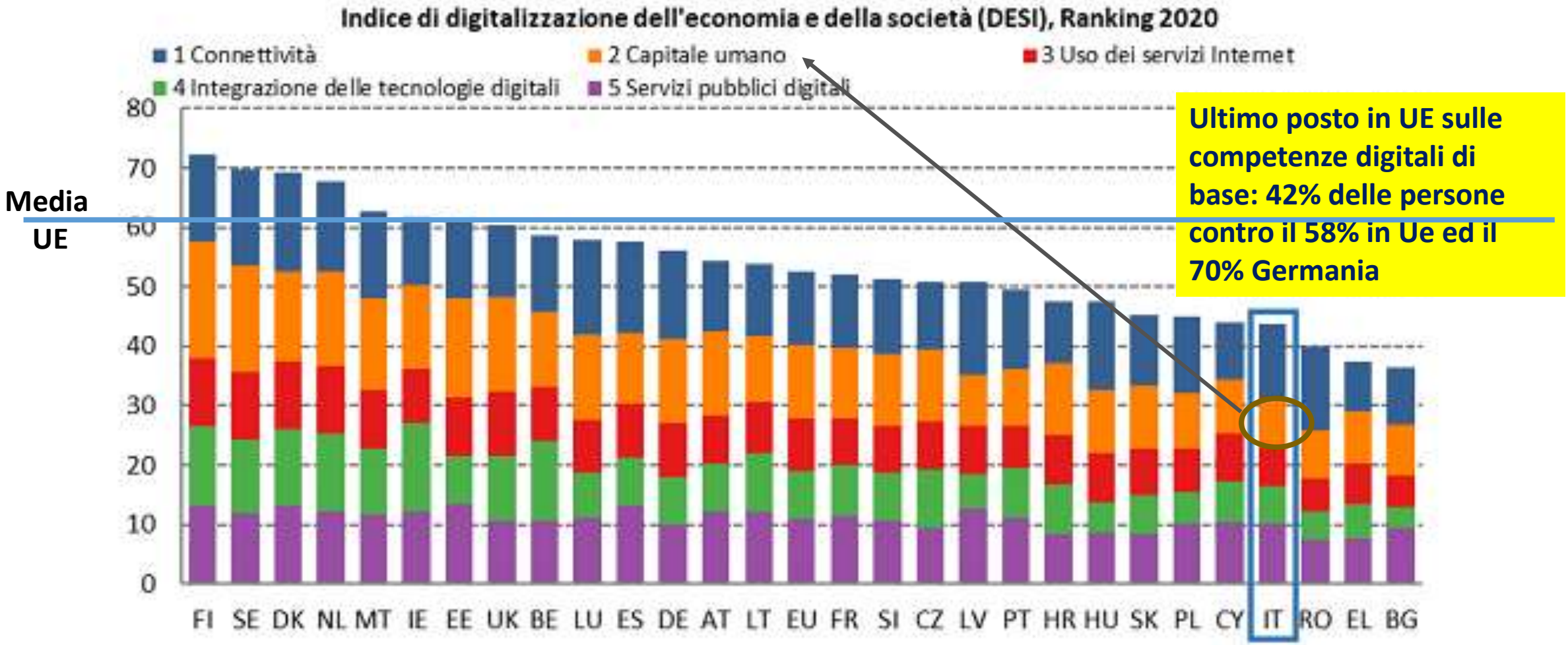
- ***Tecnica***
- ***Organizzativa***
- ***Personale***

TUTTI i sistemi ICT hanno vulnerabilità tecniche

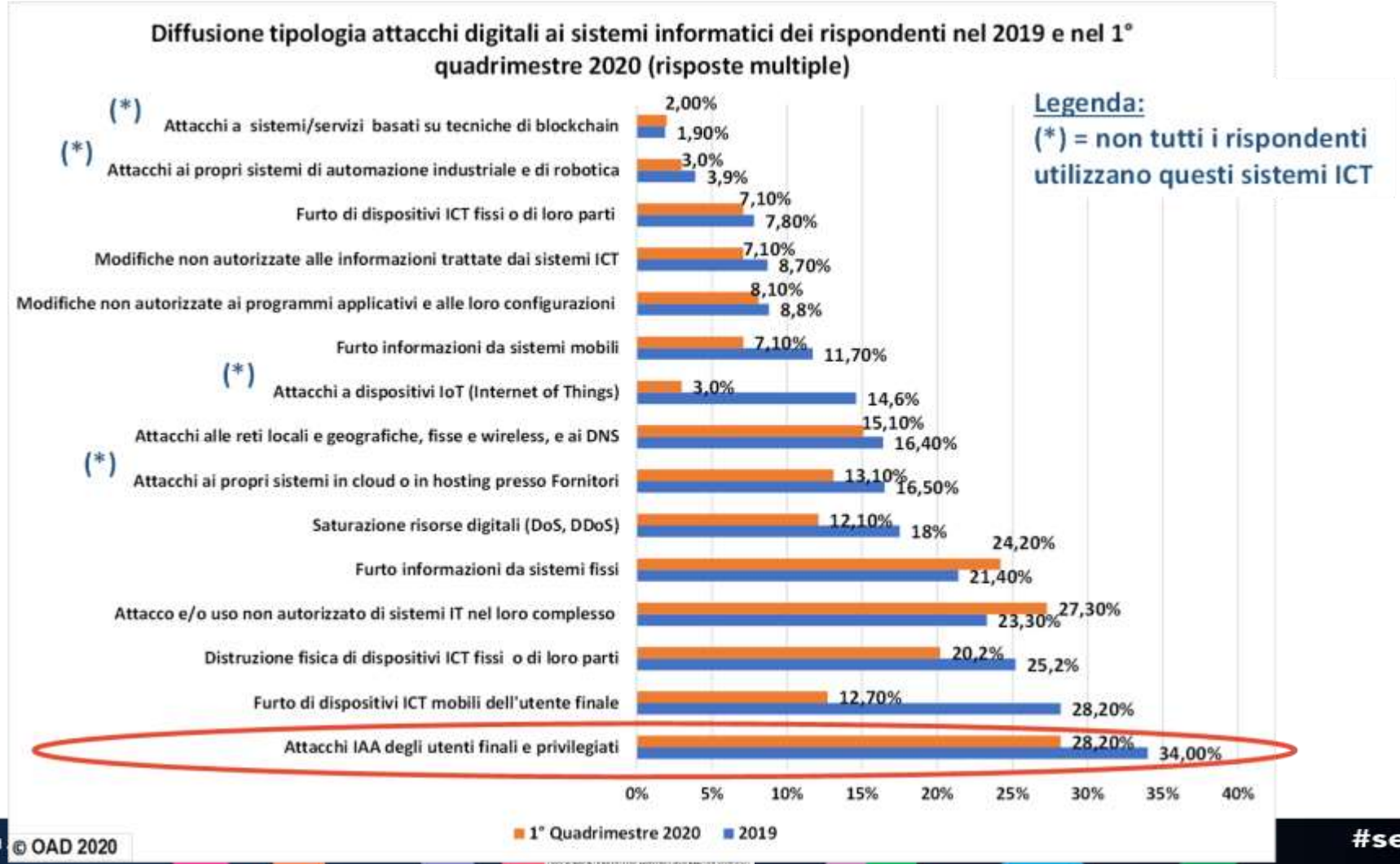


Fonte: CVE Mitre

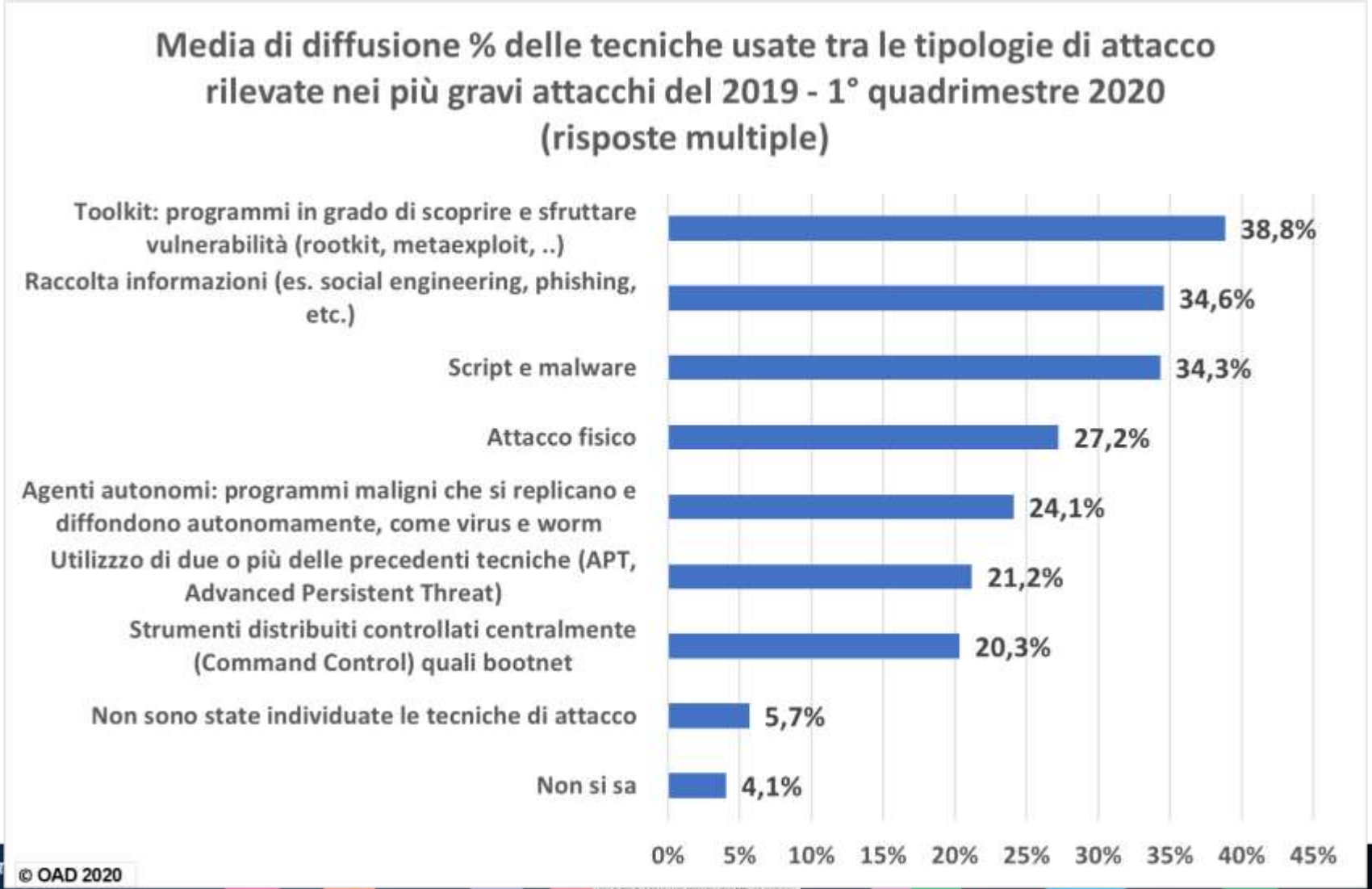
Indice europeo DESI 2020



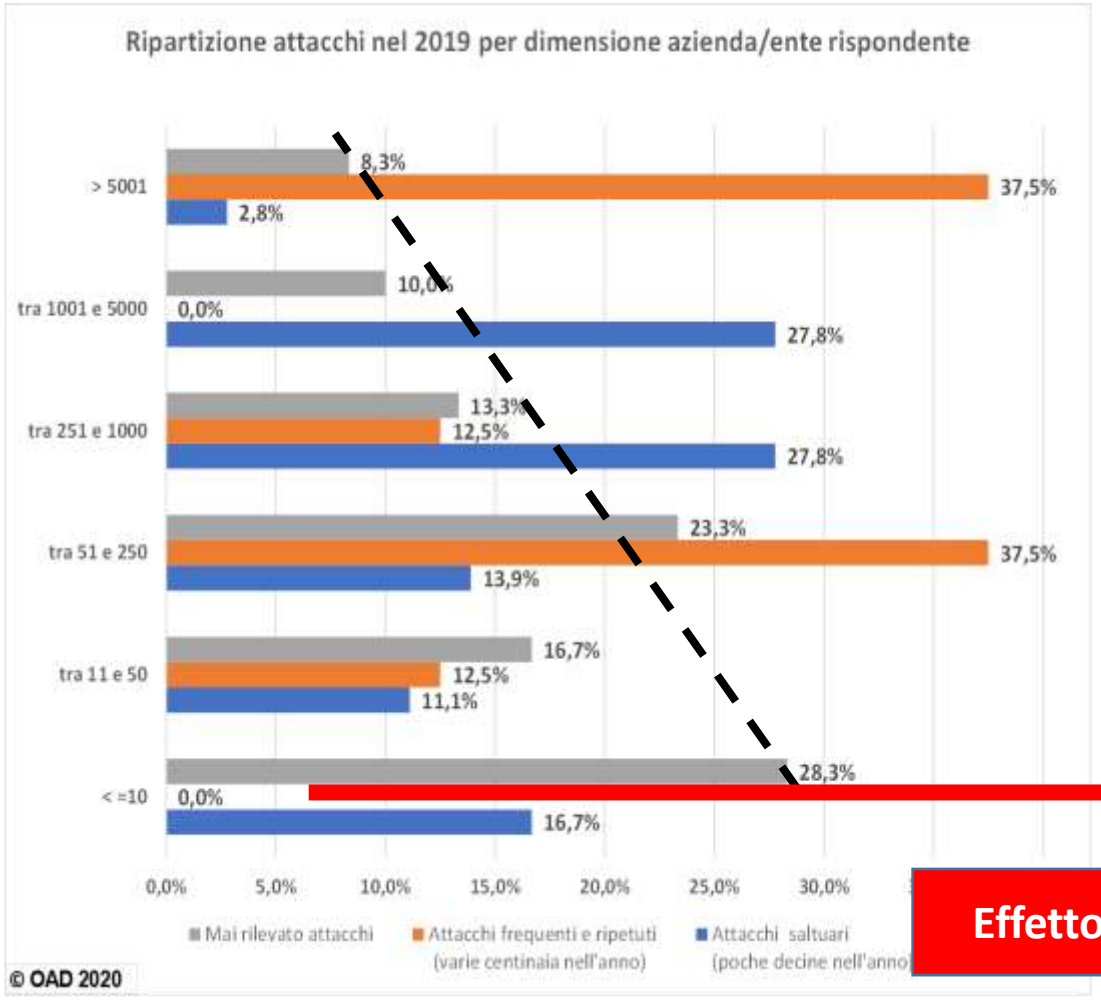
OAD 2020: diffusione % tipologia attacchi digitali (che cosa viene attaccato)

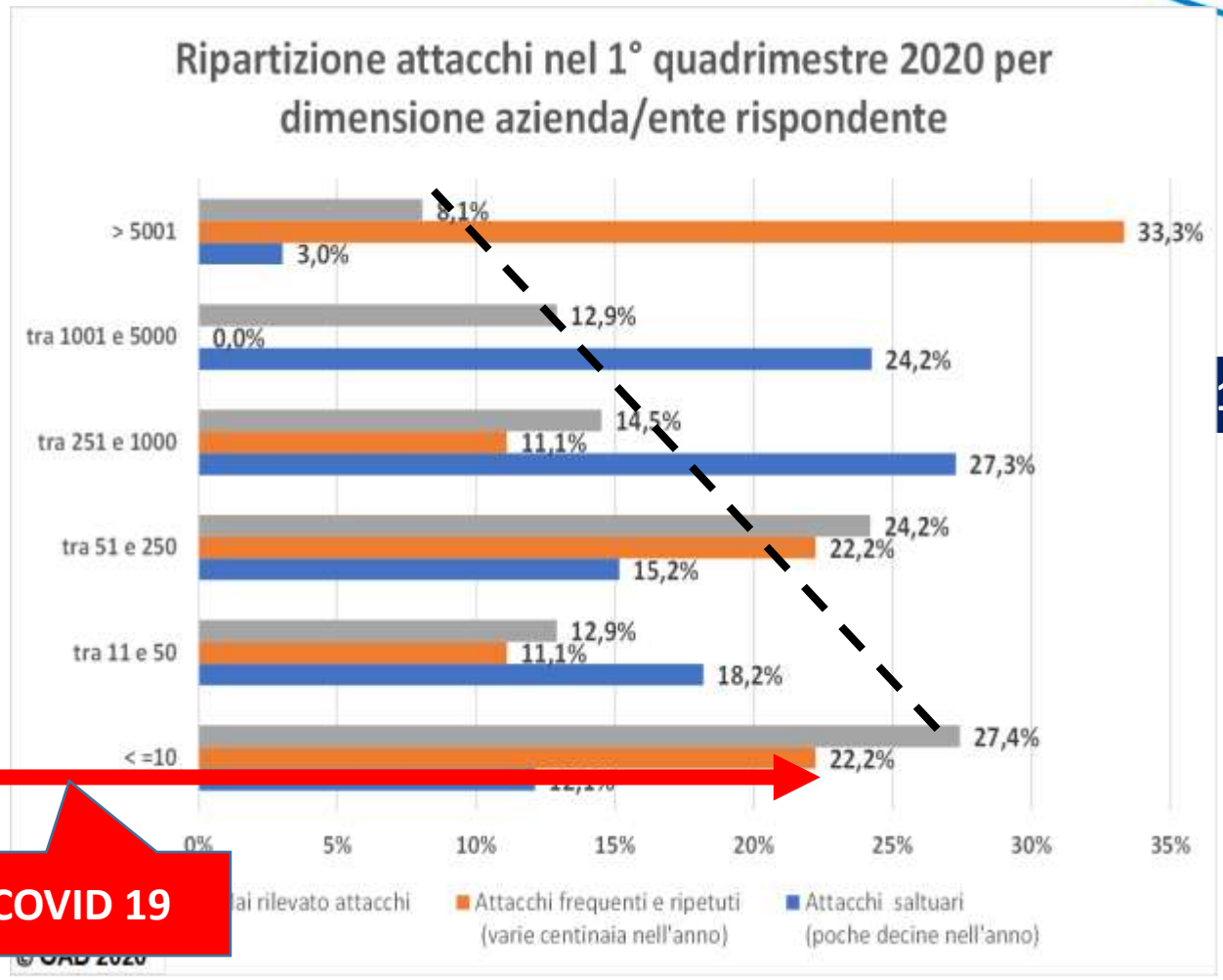


OAD 2020: Tecniche di attacco (come) più diffuse tra i rispondenti



Attacchi digitali per dimensione di Azienda/Ente





Effetto COVID 19

OAD 2020: Dai dati della Polizia Postale

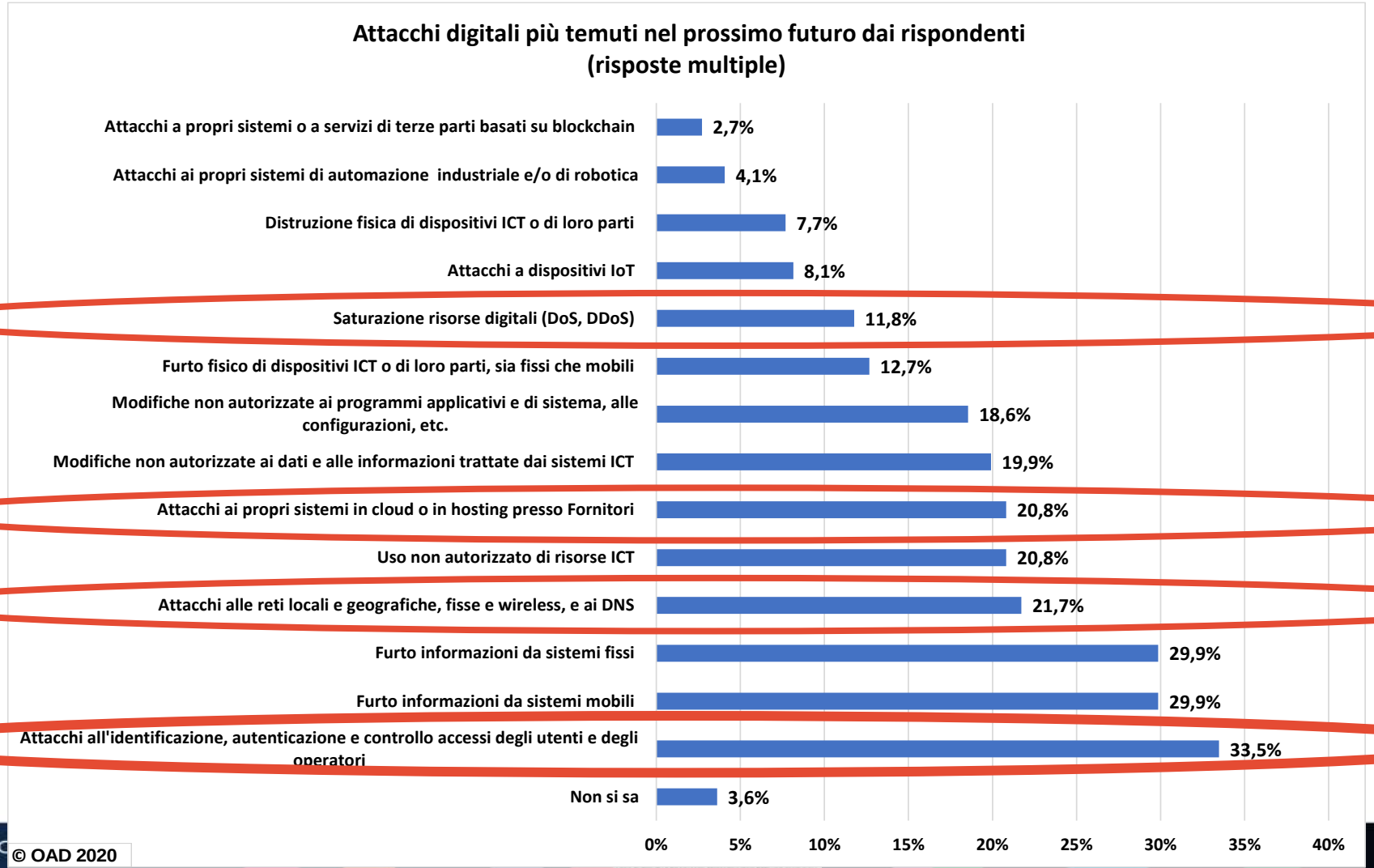
Protezione strutture critiche	1 gen - 30 apr 2020	1 gen - 31 dic 2019	1 gen – 31 dic 2018	1 gen – 31 dic 2017	1 gen – 31 dic 2016
Attacchi rilevati	282	1181	459	1.032	844
Alert diramati	24.824,00	82.484,00	80.777	31.524	6.721
Indagini avviate	34	155	74	72	70
Persone arrestate	0	3	1	3	3
Persone denunciate	0	117	14	1.316	1.226
Perquisizioni	n.d.	n.d.	n.d.	73	58
Richiesta di cooperazione internazionale in ambito Rete 24/7 High Tech Crime G8 (Convenzione Budapest)	17	79	108	83	85
Indagini avviate su attacchi rilevati	12,05%	13,12%	16,12%	6,98%	8,29%
Persone arrestate su persone denunciate	0%	2,50%	7,14%	0,23%	0,24%

Financial Cyber Crime	1 gen - 30 apr 2020	1 gen - 31 dic 2019	1 gen – 31 dic 2018	1 gen – 31 dic 2017	1 gen – 31 dic 2016
Transazioni Fraudolente Bloccate	€ 20.200.000,00	€ 21.333.990,00	€ 38.400.000,00	€ 20.839.576,00	€ 16.050.812,50
Somme Recuperate	€ 8.700.000,00	€ 18.000.000,00	€ 9.000.000,00	€ 862.000,00	nd
Arrestati		nd	nd	25	25
Denunciati		nd	nd	2.851	3.772
Recupero/frode	43,06%	84,37%	23,44%	4,14%	

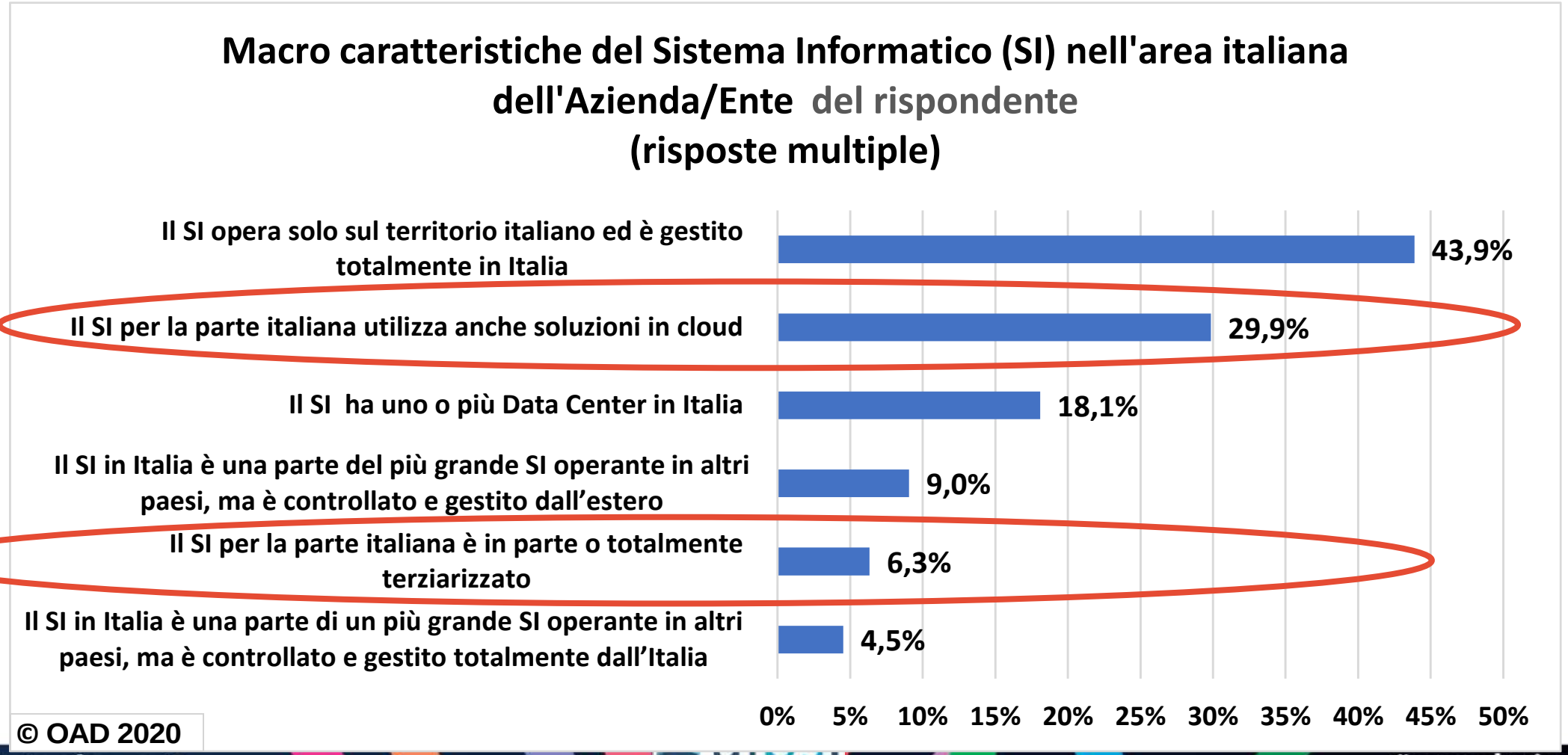
Effetto COVID 19

Cyber Terrorismo	1 gen - 30 apr 2020	1 gen - 31 dic 2019	1 gen – 31 dic 2018
Spazi web monitorati	11.962	36.377	36.000
Contenuti rimossi			250

Attacchi più temuti nel prossimo futuro dai rispondenti OAD 2020



Utilizzo di soluzioni cloud nei SI in Italia dei rispondenti OAD 2020



Le misure di sicurezza digitale implementate

OAD 2020: misure di sicurezza digitale dei rispondenti

Nel complesso nettamente migliorate rispetto alle precedenti indagini OAD

- **Misure tecniche**
  - Architettura complessiva delle misure della sicurezza digitale del sistema informatico
  - Contromisure fisiche
  - Misure di Identificazione, Autenticazione, Autorizzazione (IAA)
  - Contromisure tecniche sicurezza digitale a livello di reti locali e geografiche
  - Contromisure tecniche per la protezione logica dei singoli sistemi ICT
  - Contromisure tecniche per la protezione degli applicativi
  - Contromisure per la protezione dei dati

Migliorate, ma misure di base da potenziare soprattutto per le PMI

- **Misure organizzative**
  - Struttura organizzativa, ruoli, competenze, certificazioni
  - Policy e procedure organizzative
  - Contratti e clausole sicurezza digitale con le Terze Parti (GDPR dovrebbe aiutare!!)
  - Consapevolezza (awarness) sicurezza digitale a tutti i livelli
  - Auditing

Migliorate ma ancora carenti nelle PMI

- **Misure di gestione e di governo**
  - Sistemi di controllo, monitoraggio e gestione della sicurezza digitale
  - Piano di Disaster Recovery (DR)

Migliorate ma:
- **Carenti per PMI**
- **Embrionali per le soluzioni più avanzate (AI, ML, etc.)**
- **DR più formale che sostanziale**

Con vulnerabilità ad alta densità, le attuali misure di sicurezza sono ancora valide?

- Le tipiche **misure tecniche ed organizzative di sicurezza digitale**, **dal costo crescente**, ***sono ancora sufficienti ed efficaci?***
  - Sono **necessarie** **ma non sufficienti**, con una continua e costosa rincorsa per far fronte alle nuove vulnerabilità e ai nuovi attacchi, che in molti casi sono comunque a favore degli attaccanti
- Molti esperti, a livello mondiale, da *Dan Geer* a *Bas Alberts,* ritengono che non si debba più spendere prevalentemente per tali misure (ma sono ancora necessarie), ma investire di più in **misure per bloccare e reprimere l'hackeraggio/cyber crime**, riducendo fortemente i loro alti guadagni con pochissimi rischi → incrementare le sanzioni legali, sia civili che penali, e reale collaborazione tra le Polizie nel cybercrime
- Si dovrebbe entrare nella logica di **security by design e by default**, ossia di **sicurezza digitale intrinseca nei dispositivi e nelle applicazioni ICT**, in modo che il sistema ICT sia sicuro indipendentemente dal suo buon o cattivo uso da parte dell'utente finale.
  - Ma allo stato attuale è realmente fattibile? Alcuni passi in tale direzione sono già stati compiuti o si stanno compiendo, come indicato nella prossima slide

I principali trend tecnologici ed organizzativi per la sicurezza digitale

- **A livello tecnico**
  - Crescita del numero e dell'utilizzo, a livello mondiale, di soluzioni di "**cybersecurity as a service**" fornite dai **MSSP**, Managed Security Service Provider
  - Crescente **automazione** della gestione operativa dei SI, anche con crescente uso di strumenti di **intelligenza artificiale** e di **machine learning**
  - Crescente diffusione ed utilizzo di approcci ed architetture
    - **Microservice Architecture**, evoluzione della SOA, Service Oriented Architecture
    - **Zero-Trust Architecture**
    - **SASE**, Secure Access Service Edge
    - **SOAR**, Security Orchestration, Automation and Response
  - Nuove logiche e soluzioni per la virtualizzazione: Container, Docker, Kubernetes, …
  - Crescente diffusione di sistemi con **strumenti di sicurezza built in nell'hardware a livello di chip (trusted device)** identificazione e autenticazione utenti, protezione dati con crittografia, sicurezza BIOS, sicurezza screen, etc.
  - Nell'ambito dello **sviluppo software** crescente diffusione dell'approccio **DevOps** con piattaforme e linguaggi di programmazione intrinsecamente più sicuri
  - Accessi ai sistemi passwordless con identificazione biometrica (es FIDO2)
- **A livello organizzativo**
  - Richiesta compliance a normative europeo quali **GDPR- Regolamento UE 679/2016** per la privacy, **Direttiva UE NIS** 2016/1148 per la sicurezza delle infrastrutture ICT critiche, **Cybersecurity Act - Regolamento UE 2019_881** per il rafforzamento della sicurezza cibernetica dei sistemi informatici e delle reti

Come approcciare pragmaticamente la cybersecurity

- La sicurezza digitale è un **processo continuo (continual) multi ed interdisciplinare**
  - Le **misure di sicurezza digitale** sono sia **organizzative** sia **tecniche**, e queste ultime divengono ben presto obsolete (seguono più o meno la Legge di Moor valida per l'ICT: dopo 2-3 anni sono obsolete)
  - Le varie misure di sicurezza digitale devono essere tra loro ben bilanciate: la sicurezza complessiva è come una catena, forte quanto il suo anaello più debole
  - In tale continuo processo l'**utente**, sia finale che privilegiato, del SI deve essere il **punto chiave** e di riferimento
    - Essenziale la sua sensibilizzazione, formazione e addestramento

- La **sicurezza digitale assoluta non esiste**: per un possibile attacco, **il problema non è SE ma QUANDO** e che **IMPATTI** potrà avere

- **Contestualizzare** misure tecniche ed organizzative alla propria realtà

- **Le medie e piccole realtà NON possono**, nella stragrande maggioranza dei casi, avere e mantenere al proprio interno le **competenze** necessarie per realizzare e gestire un idoneo sistema di sicurezza digitale. Devono quindi nella maggior parte dei casi **terziarizzare** sia la progettazione sia l'implementazione e la gestione operativa a Terze Parti, che siano effettivamente efficaci ed efficienti
  - Se si terziarizza, **si deve controllare quello che il Fornitore attua**, magari con l'aiuto di un autorevole e fidato consulente/Terza Parte

Come effettuare il rightsourcing? Qualche suggerimento pratico

- **Verificare la reputazione** delle Terze Parti considerate: contattare il vertice di qualche loro cliente dello stesso settore e di analoghe dimensioni/necessità, vedere il loro sito web, i social nets, articoli pubblicati, etc.

- Richiedere e verificare con le Terze Parti coinvolte:
  - **Che facciano riferimento ai principali standard e alle best practices ben consolidate: OSA, ITIL v3, Cobit, ISO 27000, NIST SP, …**
  - Che seguano un **approccio proattivo** e **adattativo**
  - Che effettuino una buona **analisi delle vulnerabilità, dei rischi e degli impatti**
  - Che prevedano e seguano un **approccio architetturale ben bilanciato** tra le varie misure tecniche ed organizzative, tenendo anche conto delle misure già in essere
  - Verificare i **contratti** e le loro **SLA e KPI**
  - Verificare il **rapporto prestazioni/prezzo** (considerando almeno due-tre interlocutori diversi)

- Se digiuni di cybersecurity, scegliere (con i criteri di cui sopra) ed affidarsi ad un consulente o Terza Parte come **coordinatore** e **supervisore** di cosa attuano, e come, i Fornitori, assicurandosi che sia realmente **indipendente dai Fornitori**

GRAZIE DELL' ATTENZIONE e …

- Le slide di questa presentazione saranno scaricabili dal sito AIPSI e OAD
- Segua i prossimi **webinar AIPSI**
- Si iscriva alla **newsletter AIPSI** mensile
- Se interessato alla sicurezza digitale, **è ora di iscriversi ad AIPSI!**
- Per contattare l'associazione : aipsi@aipsi.org
- Marco R. A. Bozzetti: m.bozzetti@aipsi.org