Mind the Gap

Il differenziale retributivo dell'Italia nelle retribuzioni degli esperti in cybersecurity

Gennaio 2023

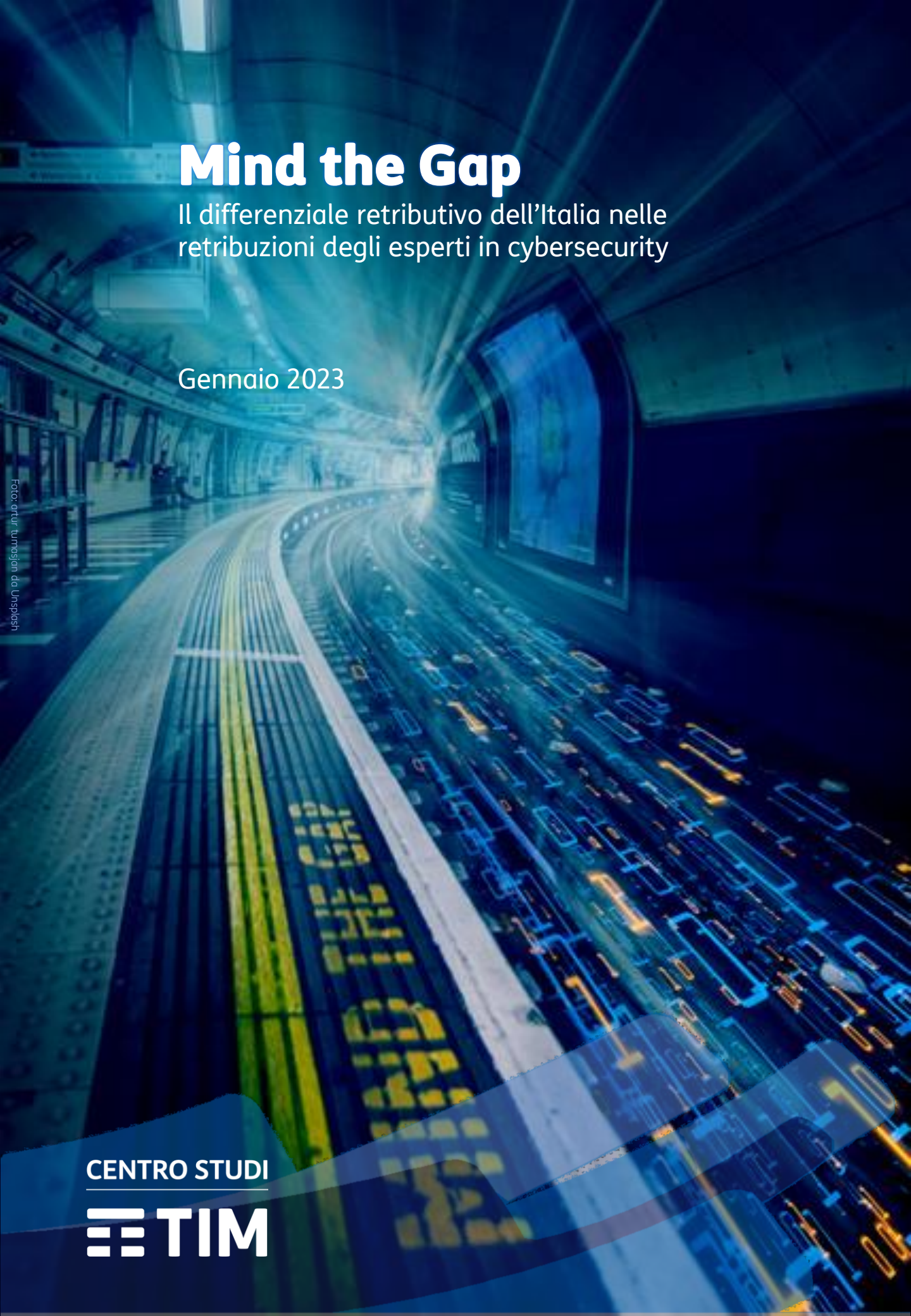


Foto: artur tumasjan da Unsplash

CENTRO STUDI

TIM

Scenario

IL COSTO DEGLI ATTACCHI CYBER

La progressiva digitalizzazione porta benefici indubbi, ma allo stesso tempo amplia la superficie di attacco potenziale e rende necessario aumentare ancora di più la consapevolezza di imprese, istituzioni e cittadini verso il rischio di un attacco cyber.

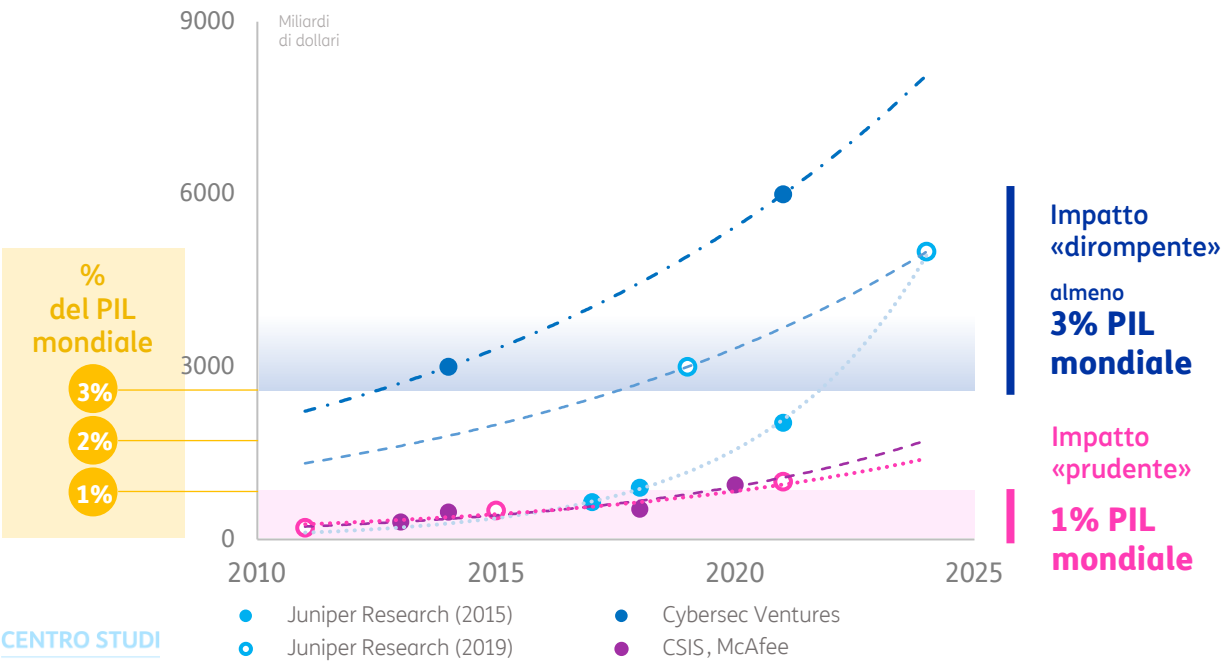
Il rischio cyber è una minaccia costante, dalla capacità d'impatto elevata e non ancora interamente compresa. Secondo le analisi del World Economic Forum (WEF), il rischio legato agli attacchi cyber si colloca da sempre tra le prime 10 minacce globali che possono incidere negativamente sull'equilibrio del sistema socioeconomico e politico mondiale. Negli ultimi 10 anni, i cyber attacchi non sono mai usciti dal radar dei maggiori rischi, mostrando una presenza costante e continua.

Secondo gli scenari più «prudenti», il costo della minaccia cyber è di almeno 1% del PIL Mondiale

Per altri Osservatori, l'impatto è almeno 3 volte superiore, perché alcuni incidenti informatici non sono dichiarati, spesso non vi è consapevolezza piena del danno subito oppure perché possono cambiare i perimetri delle stime.

(es. alcuni studi includono danni immateriali sulla reputation aziendale, impatto della perdita di informazioni coperte da intellectual property, ecc.).

Impatto economico degli attacchi informatici nel mondo. Diversi scenari a confronto



CENTRO STUDI TIM

Fonte: Elaborazione Centro Studi TIM

I FRONTI CALDI

Secondo l'ultimo rapporto Clusit (novembre 2022), gli attacchi gravi sono aumentati del 53% tra il 2018 ed il 2022, passando da una media mensile di 124 a 190 episodi. La crescita non riguarda solo la frequenza, ma anche la severità degli attacchi che diventa di anno in anno sempre più importante. Nei primi sei mesi del 2022 un attacco su tre è stato classificato come critico.

La principale motivazione di attacco è lo sfruttamento economico, ma sempre più spesso, anche a causa della tensione internazionale dovuta al conflitto russo-ucraino in corso, sono in aumento le azioni rivolte verso bersagli specifici che rappresentano dei punti vitali del'organizzazione di un Paese: infrastrutture critiche, sistemi sanitari, obiettivi governativi e militari.

Del resto, anche il World Economic Forum evidenzia, nel Global Risk Report del 2022, che la dimensione cibernetica è un nuovo terreno di scontro su cui possono esplodere gli interessi divergenti dei Paesi, facendo prevalere le visioni unilaterali rispetto alla cooperazione.

ATTACCHI ALL'EUROPA

In 6 mesi del 2022

26%
attacchi rivolti verso Europa, in diminuzione quota attacchi America e Asia.

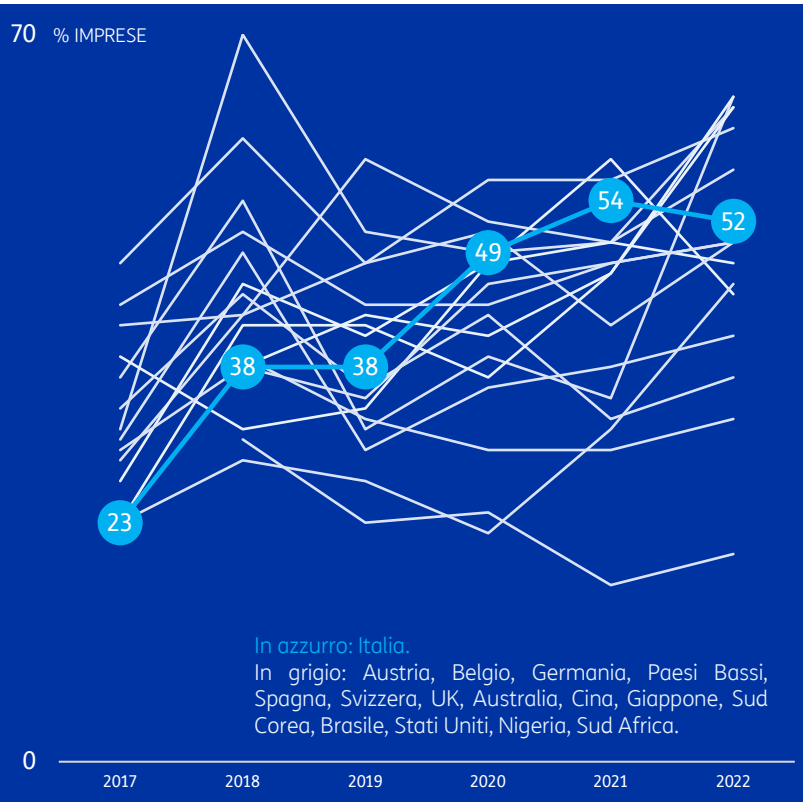
BERSAGLI PREVALENTI

>40%
di attacchi indirizzati a obiettivi governativi e/o militari, sistemi informatici, sanità.

Fonte: CLUSIT novembre 2022

I TIMORI DELLE IMPRESE

Negli ultimi anni, la minaccia di incidenti informatici si è progressivamente estesa a tutte le tipologie di aziende, non solo grandi operatori, ma anche imprese di piccola e media dimensione che hanno sistemi di difesa più penetrabili e possono anche rappresentare un veicolo per insinuarsi tra le maglie di difesa di imprese clienti di dimensioni più grandi.



In azzurro: Italia.
In grigio: Austria, Belgio, Germania, Paesi Bassi, Spagna, Svizzera, UK, Australia, Cina, Giappone, Sud Corea, Brasile, Stati Uniti, Nigeria, Sud Africa.

Fonte: Allianz Risk Barometer – vari anni

ALL'INCIRCA 1 AZIENDA ITALIANA SU 2 TEME UN ATTACCO CYBER

Nel corso del tempo è aumentata la percezione del rischio di incidenti informatici ed attacchi cyber a scopo estorsivo tra le imprese italiane. I rapporti realizzati dal gruppo assicurativo Allianz sui rischi a cui è esposta un'azienda mostrano tale crescita: nel 2017 meno di un'azienda su quattro segnalava timori per un attacco cyber, nel 2022 tale quota era salita a oltre il 50%.

In questo scenario di minaccia crescente, la difesa dei dati è uno dei fronti critici. Sempre più spesso si rivolgono a fornitori specializzati di servizi cloud che possono garantire sistemi di sicurezza più robusti.

LA CRESCITA DELLA SPESA IN CYBERSECURITY

+11%

Incremento del budget 2023 per la spese in sicurezza e gestione del rischio a livello mondiale.

+27%

incremento del budget 2023 per sicurezza dei sistemi cloud a livello mondiale.

Fonte: Gartner

CENTRO STUDI TIM

CYBERDIFESA: UN TEMA DI COMPETENZE

Per rinforzare le strutture di cyberdifesa in Italia, uno degli aspetti chiave è quello della formazione delle competenze, dell'attrazione dei talenti, della capacità di trattenere risorse esperte e qualificate. A livello mondiale l'associazione noprofit (ISC)² stima che ci sia una carenza di circa 3,4 milioni di esperti in cybersecurity e secondo Fortinet 6 aziende su 10 a livello mondiale affronta incontra difficoltà nel trovare risorse preparate.

A LIVELLO GLOBALE

3,4 milioni
di cyberesperti in meno rispetto alle necessità

6 aziende su 10
incontra difficoltà nel trovare esperti in cybersecurity

EUROPA

L'ENISA, l'agenzia europea per la cybersecurity mette in guardia sulla carenza di esperti che può diventare **UNO DEI PUNTI CRITICI** del sistema di difesa europeo

ITALIA

Secondo ACN, l'Agenzia per la Cybersicurezza Nazionale, in Italia si stima una carenza di circa **100MILA ESPERTI** in cybersecurity per coprire le esigenze di imprese e PA

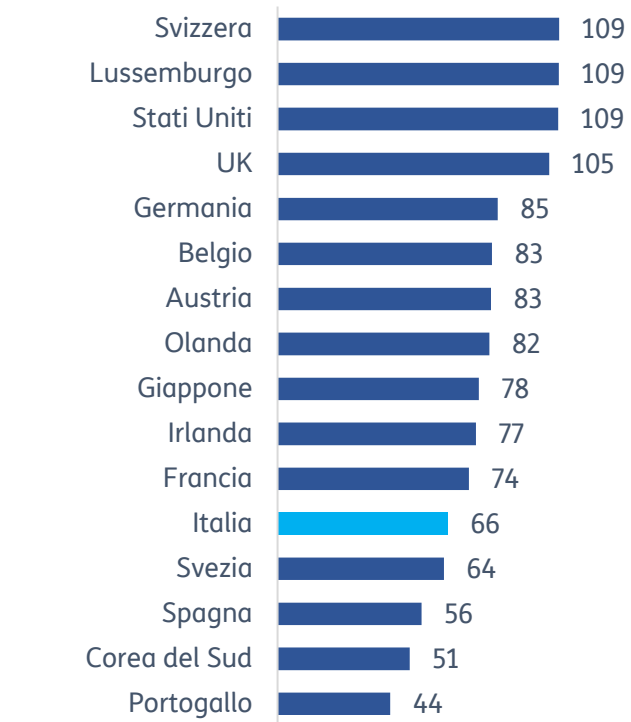
Il gap retributivo dell'Italia

IL CYBERSECURITY SPECIALIST

Le principali attività di un Cybersecurity Specialist

Prevenzione e protezione. Identifica e risolve problemi di elevata complessità per prevenire attacchi informatici ai sistemi informativi e per proteggere i sistemi informatici da interruzione del servizio, furto di proprietà intellettuale, virus di rete, data mining, furto finanziario e furto di dati sensibili dei clienti.
Monitoraggio. Progetta, installa e gestisce meccanismi di sicurezza che proteggono reti e sistemi informativi da hacker, violazioni, virus e spyware.
Risposta. Risponde agli incidenti, indaga sulle violazioni e consiglia miglioramenti per colmare potenziali lacune nella sicurezza.

Retribuzione lorda media in Paesi selezionati 2021
migliaia di euro



Fonte: Economic Research Institute

Nel 2021, la retribuzione lorda annua di un cybersecurity specialist, con un profilo di esperienza medio, era pari a circa 66 mila euro in Italia. Svizzera, Lussemburgo, USA e UK hanno retribuzioni lorde che superano i 100 mila euro.

Nota: per UK si riporta la retribuzione di un occupato a Londra. Per gli USA è stata presa la retribuzione di un occupato nella zona di New York / Manhattan.
Le valutazioni considerano il solo stipendio base senza considerae eventuali retribuzioni variabili.

CONFRONTO REALE

Per effettuare un confronto reale tra i livelli retributivi bisogna tenere conto degli effetti legati al diverso livello di tassazione ed al costo della vita

CUNEO FISCALE

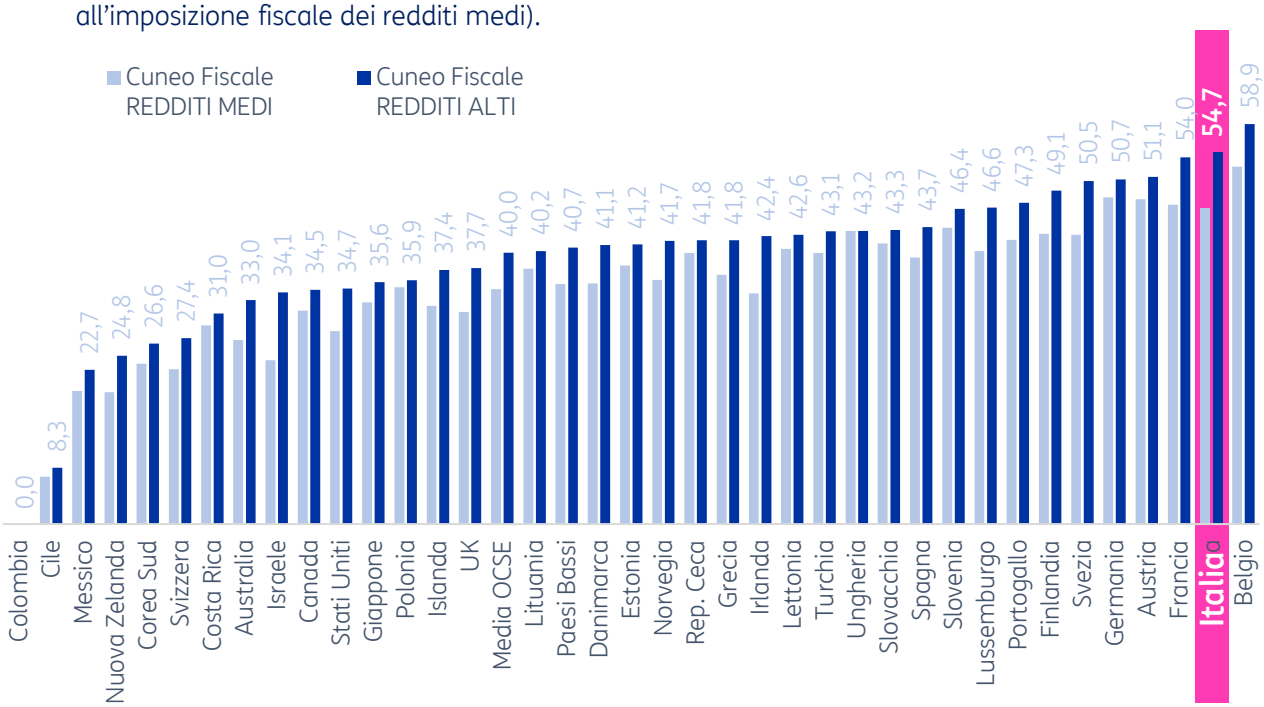
COSTO DELLA VITA

Nei Paesi selezionati vigono differenti sistemi di tassazione del lavoro e questo influisce sulla determinazione del netto percepito dal singolo cybersecurity specialist.

Il confronto deve tenere conto del differente costo della vita presente nei diversi contesti esaminati, valutando il potere di acquisto delle retribuzioni dei cybersecurity specialist.

L'Italia ha un cuneo fiscale elevato, in particolare per i redditi alti

L'Italia ha uno dei cunei fiscali più elevati a livello OCSE, in particolar modo per i redditi elevati, in cui ricade la retribuzione media di un cybersecurity specialist in quasi tutti i Paesi esaminati, ad eccezione di alcuni casi (ad esempio, in Svizzera, la retribuzione sarebbe soggetta all'imposizione fiscale dei redditi medi).



CENTRO STUDI TIM

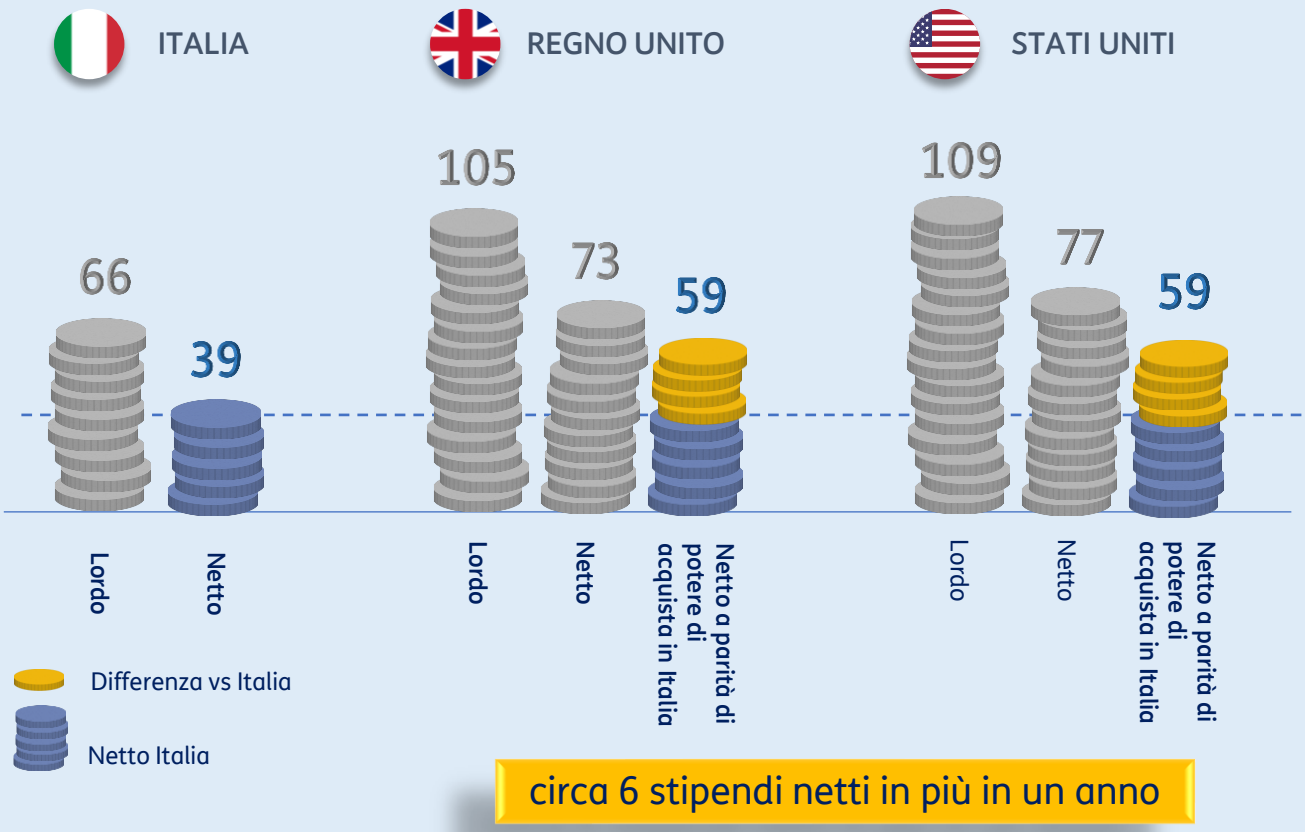
Fonte: OCSE Taxing Wages 2022. Si considerano elevate le retribuzioni lorde che eccedono del 67% la retribuzione lorda media calcolata dall'OCSE per ogni singolo Paese.

DIFFERENZIALE RETRIBUTIVO CON USA E UK

In USA e UK la tassazione incide meno sulla retribuzione del lavoratore rispetto all'Italia, ma il costo della vita è più elevato. Il confronto effettuato a parità di potere di acquisto dell'Italia mostra un differenziale reale di circa 20mila euro.

€ migliaia e €PPP per i confronti a parità di potere di acquisto

Fonte: elaborazione su dati OCSE, Economic Research Institute e PPP Salary Converter



circa 6 stipendi netti in più in un anno

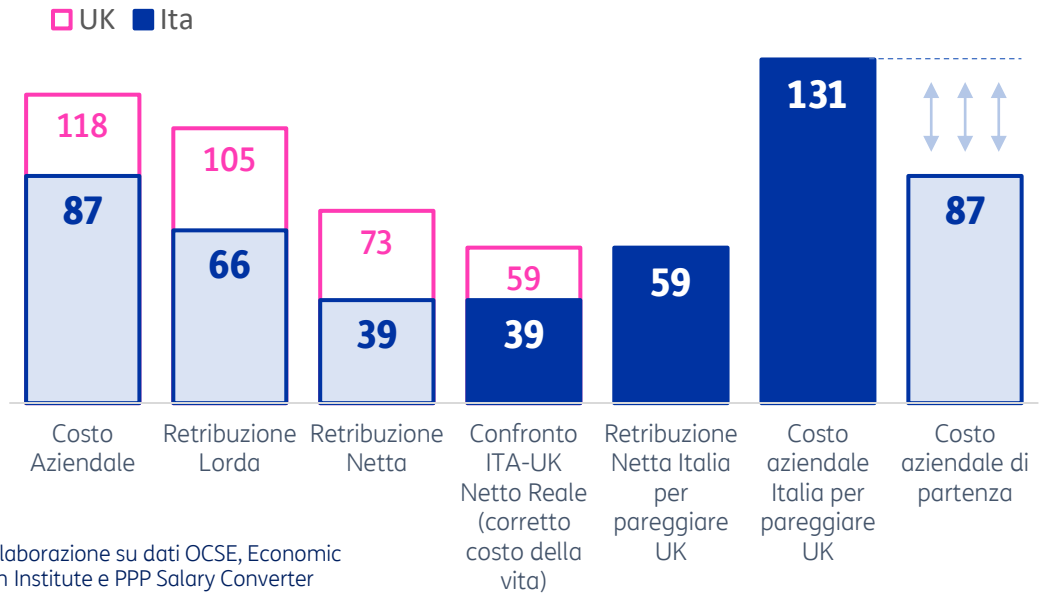
LA VARIANTE SMART WORKING

Nel caso in cui un cybersecurity specialist potesse lavorare in tutto o in parte in modalità smart, il lavoratore continuerebbe a godere del costo della vita italiano. Un cybersecurity specialist assunto da una azienda di Londra in modalità smart working guadagnerebbe quasi il doppio della retribuzione netta italiana media.

MIND THE GAP:
IL PUNTO DI VISTA DELLE AZIENDE

Dal punto di vista si un'impresa di italiana, per pareggiare l'offerta di lavoro ad uno specialista in cybersecurity proveniente da una concorrente inglese, significa incrementare il costo aziendale del 50%

Quale costo aziendale deve sostenere un'azienda di cybersecurity italiana per pareggiare l'offerta economica di una concorrente inglese



Fonte: elaborazione su dati OCSE, Economic Research Institute e PPP Salary Converter

Questa situazione può anche essere letta in un altro modo. Se un'azienda italiana avesse bisogno di 150 cybersecurity specialist, dato un budget di spesa fissato, potrebbe riuscirne a pagare solo 100 al prezzo del Regno Unito

Appendice

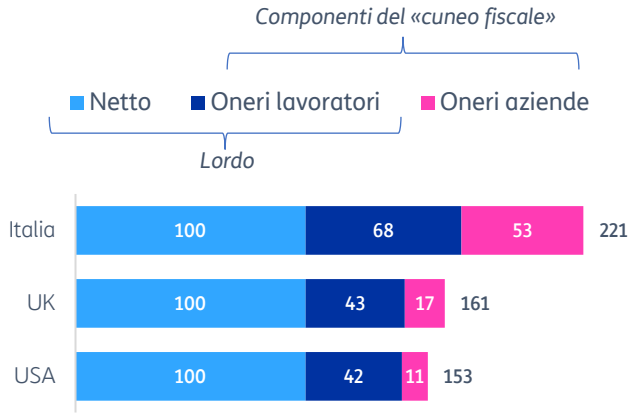
UNO ZOOM SUL CUNEO FISCALE

Il cuneo fiscale è un fattore difficile da comprendere perché è riferito al costo complessivo del lavoratore per l'azienda che è poco noto. Cambiando punto di riferimento e rapportando le diverse voci alla retribuzione netta, si evidenzia quanto pesa tale componente. Un lavoratore ha un costo aziendale pari a 2,2 volte la retribuzione netta in Italia, mentre in USA e UK tale valore è tra 1,5 ed 1,6 volte.

Gli oneri fiscali per le imprese sono la metà della retribuzione netta

Componenti del costo aziendale in base alla retribuzione netta
(Numero Indice, Retr. Netta = 100)

Se rapportiamo il cuneo fiscale alla retribuzione netto, ci rendiamo conto che, per i redditi elevati, il cuneo fiscale in Italia rappresenta una componente superiore allo stesso reddito e gli oneri a carico delle aziende sono circa la metà della retribizione netta



Fonte: elaborazione su dati OCSE Taxing Wages 2021
Nota: Elementi quali TFR e contributi INAIL non considerate nei parametri di confronto OCSE.