CYBERSECURITY MADE IN ITALY

CENTRO STUDI

TIM

Centro Studi TIM

Roma, 20 giugno 2023

Indice

PREMESSA

Il rischio cyber per le imprese: una panoramica a livello globale

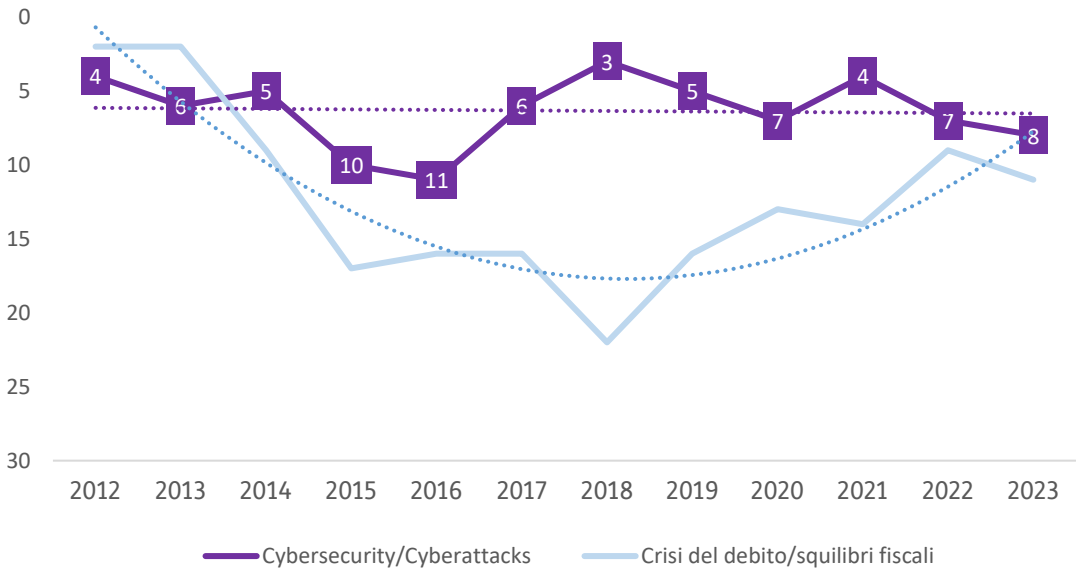
La minaccia di attacchi cyber: una costante presente da oltre un decennio tra i principali rischi a livello internazionale

Nel 2010, quando erano ancora vivi gli echi della crisi finanziaria del 2008 e le criticità sul fronte economico e geopolitico destavano le maggiori preoccupazioni a livello internazionale, gli attacchi rivolti ai sistemi e alle infrastrutture informatiche erano considerati dagli esperti del World Economic Forum come un rischio da iniziare a monitorare. Nel Global Risk Outlook dell'anno successivo si riconosceva che stava "crescendo la consapevolezza che il mondo reale" fosse "vulnerabile alle minacce alla sicurezza provenienti dal mondo virtuale" ma che "la complessità delle questioni di sicurezza informatica non era ancora ben compreso e i rischi potevano essere sottovalutati".

A differenza delle altre tipologie di rischio che, a seconda degli andamenti economici globali o delle tensioni geopolitiche, mostrano delle dinamiche cicliche o comunque compaiono in modo non continuativo tra le principali fonti di preoccupazione, il tema degli attacchi cyber è rimasto stabilmente nella "top ten" dei rischi più probabili / imminenti fin dall'inizio della scorsa decade.

Figura 1 - Gravità relativa dei rischi

Posizione nel ranking



Fonte: World Economic Forum Global Risks Perception Survey 2022-2023

A testimonianza del fatto che si tratta di un rischio concreto con impatti diretti e immediati sull'attività produttiva, oggi sono proprio i manager delle imprese che lo percepiscono in maniera ancora più netta e marcata: quest'ultimi, infatti, includono l'eventualità di un attacco cyber al 4° posto tra i rischi a breve termine, mentre per gli esponenti del mondo istituzionale e governativo questo tema si colloca al 9° posto, superato da aspetti più presenti nel dibattito sociale, economico e politico.

Figura 2 – Gravità dell'impatto a breve termine (2 anni) per categoria di stakeholder

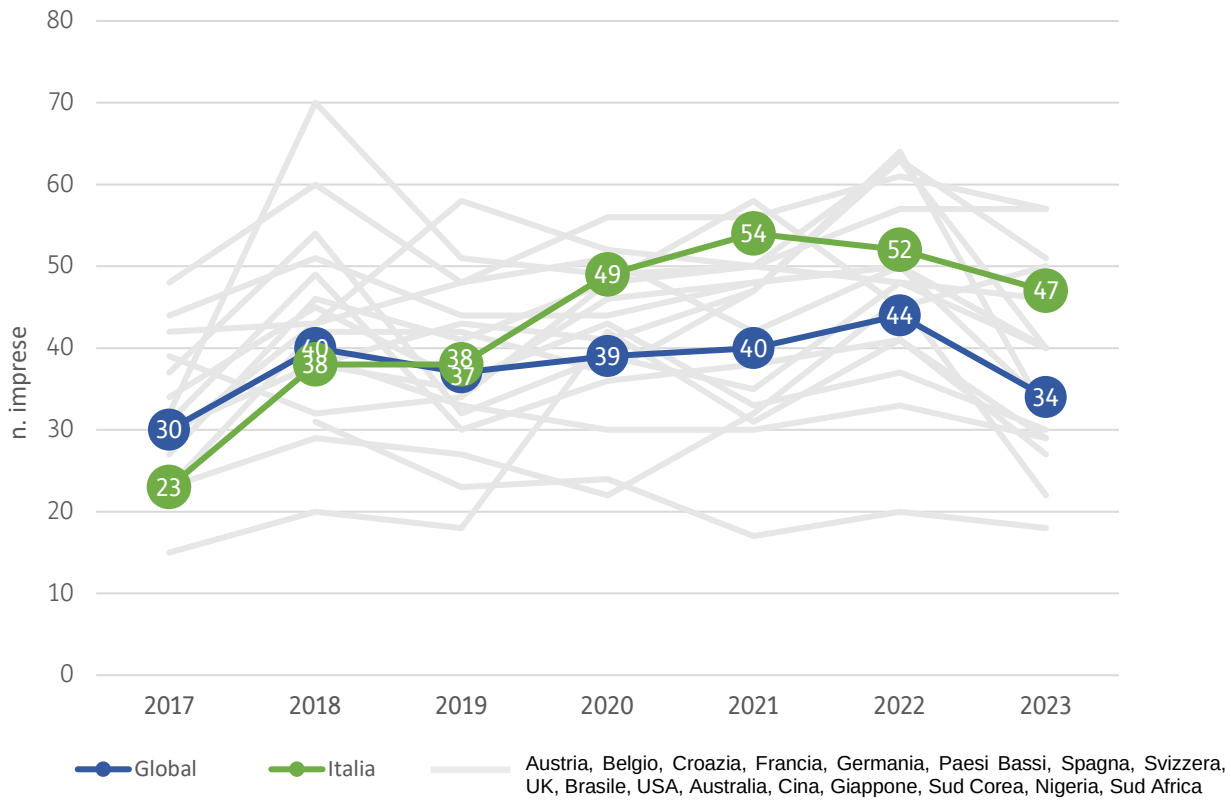
Fonte: World Economic Forum Global Risks Perception Survey 2022-2023

La percezione dei rischi legati ad attacchi cyber in Italia si è affermata in maniera rilevante e con forza crescente dal 2017

La forte preoccupazione del mondo delle imprese emerge anche da altre fonti, come ad esempio nell'indagine che viene effettuata annualmente dal gruppo Allianz, uno dei principali attori europei e mondiali del settore assicurativo, in merito ai principali rischi d'impresa. L'indagine del 2023, realizzata intervistando imprese da oltre 94 paesi, ha confermato al primo posto il rischio di incidenti legati alla sicurezza informatica per il secondo anno consecutivo. In generale, resta forte l'attenzione delle imprese verso situazioni che possono scaturire da attacchi cyber (esfiltrazioni di dati, attacchi *ransomware* che portano al blocco dell'attività con una richiesta di riscatto, incidenti causati dalla scarsa sicurezza della catena di fornitura), seppure si evidenzia un calo in termini di risposte raccolte rispetto agli anni della pandemia.

Il grafico sotto riportato mostra l'andamento della percezione del rischio cyber negli ultimi anni per una quindicina di Paesi. Come si può osservare, anche in Italia la consapevolezza dei rischi derivanti da possibili attacchi ai sistemi informatici è andata via via a consolidandosi tra i manager d'impresa a partire dal 2017. Nonostante il calo osservato a livello internazionale, dal 2020 l'Italia si colloca al

Figura 3 - Imprese che dichiarano di temere un incidente cyber (%)



Fonte: Allianz Risk Barometer – Vari anni

di sopra della media ed ancora oggi circa 1 impresa su 2 ritieni che gli incidenti informatici rappresentino un rischio.

Sebbene la rilevanza e il diffondersi del fenomeno degli attacchi informatici non conosca confini e anzi la probabilità di arrecare danni risulti maggiore laddove le imprese e le istituzioni sono meno preparate, i sistemi industriali dei diversi paesi presentano una certa inerzia e i tempi necessari per una reale presa di consapevolezza possono variare anche di molto e sostanzialmente dipendono da ragioni di natura culturale, manageriale e/o di dimensione media del tessuto produttivo . Quello che però si riscontra è che, una volta che il rischio cibernetico inizia ad affermarsi, la presa di consapevolezza rimane e, nelle imprese in cui il livello di attenzione è cresciuto, tende a rimanere alto o a crescere ulteriormente.

IL MERCATO

Accelerazione

IL MERCATO

Accelerazione

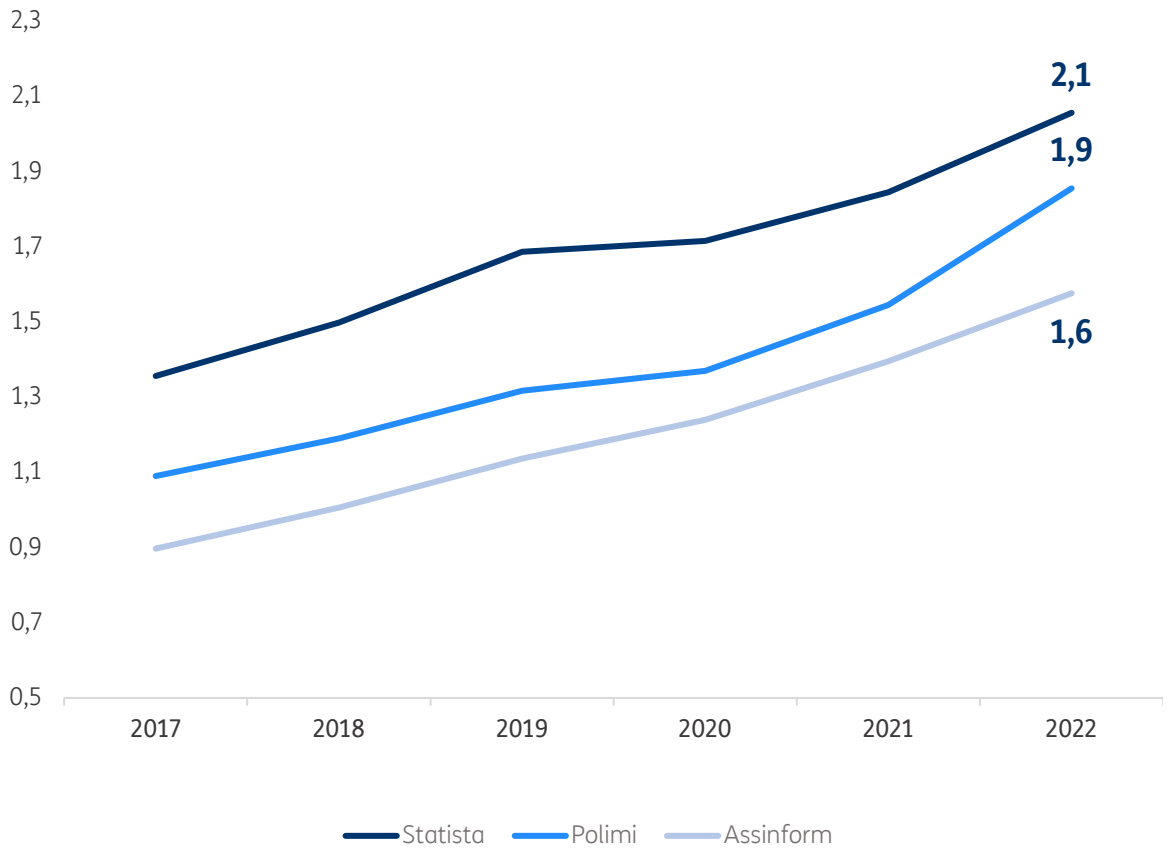
Un settore in rapida espansione

In Italia il settore della cybersecurity è in rapida espansione. Secondo le ultime ricerche dell'Osservatorio Cybersecurity & Data Protection della School of Management del Politecnico di Milano, nel 2022 si è registrata una crescita del 18% del fatturato complessivo del settore, che segue una analoga crescita a due cifre fatta registrare nell'anno precedente (+15%).

In termini di valore, il mercato italiano è stimato – a seconda delle fonti – tra gli 1,6 ed i 2,1 miliardi di euro. Le stime degli osservatori nazionali sono più cautelative, ma mostrano una crescita più intensa.

Figura 4 – Il valore del mercato italiano della Cybersecurity

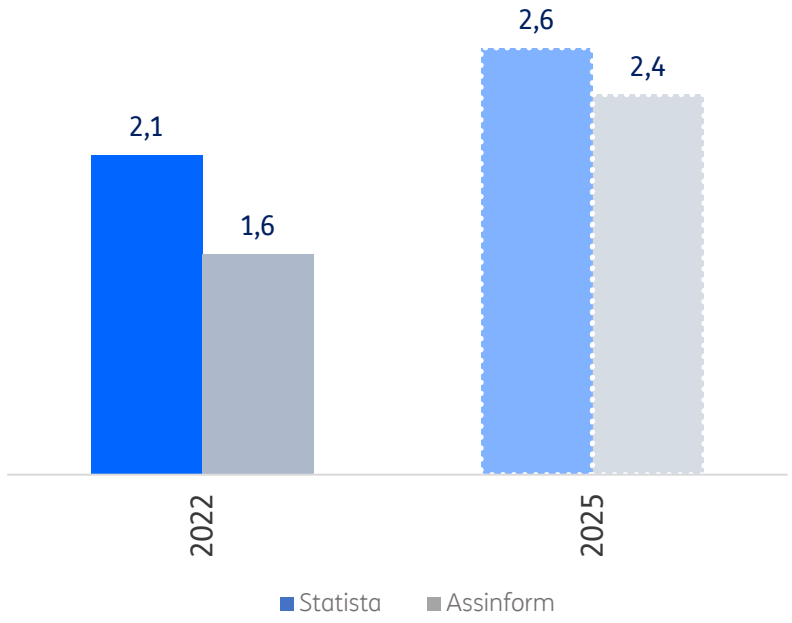
Mld €



Fonte: Statista, Osservatorio Cybersecurity & Data Protection della School of Management del Politecnico di Milano, Assinform

In termini di previsioni, si stima che al 2025 il mercato dovrebbe raggiungere un valore attorno ai 2,5 miliardi di euro, con una crescita media annua che oscilla tra 8% e il 14%. La forte crescita rilevata dall'Osservatorio della School of Management del Politecnico di Milano per il biennio 2021-2022 lascia ipotizzare una accelerazione più intensa rispetto ai valori minimi delle previsioni e che possiamo collocare attorno al 11-12% di crescita media annua per il prossimo triennio.

Figura 5 – Stima del valore del mercato italiano al 2025

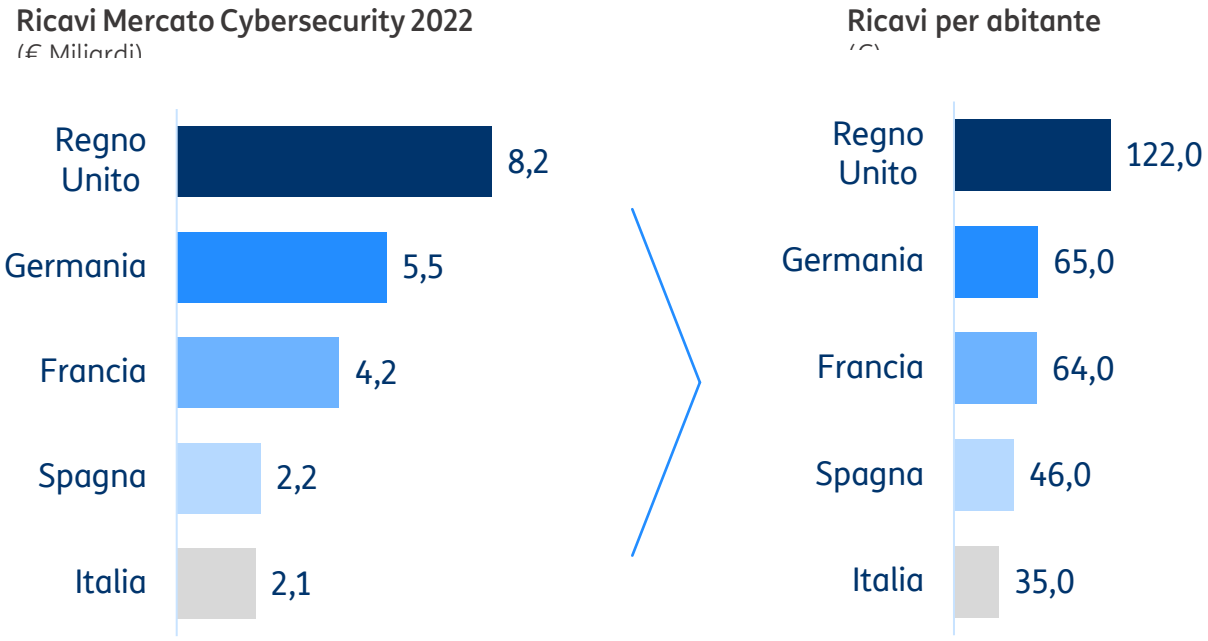


Fonte: Statista, Assinform

In effetti, la crescita degli attacchi rappresenta il principale fattore di crescita del mercato e la crescente digitalizzazione delle imprese italiane, accentuata a partire dal 2020 per far fronte alla minaccia della pandemia di Covid-19, ha aumentato la superficie d'attacco. Anche il Clusit, l'Associazione italiana per la sicurezza informatica rileva una forte progressione: gli incidenti di sicurezza informatica che hanno interessato il campione osservato dal Clusit in Italia sono aumentati del +527% con una crescita che ha superato la tendenza osservata nei quattro anni precedenti.

Nonostante l'importante crescita osservata negli ultimi anni, il mercato italiano registra ancora un forte ritardo rispetto ad altri contesti europei. Prendendo a riferimento il valore più alto di stima del mercato, il ricavo medio per abitante è di circa 35 euro in Italia, 46 euro in Spagna, circa 65 euro in Francia e Germania, 122 euro nel Regno Unito. Un divario molto significativo da colmare, ma allo stesso tempo un'importante opportunità di crescita per gli operatori del settore. In effetti, se anche in Italia si dovesse raggiungere lo stesso livello di ricavi per abitante del Regno Unito, il valore del mercato supererebbe i 7 miliardi di euro, ossia dalle 3 alle 4 volte il valore attuale.

Figura 6 – I mercati della Cybersecurity nei principali Paesi europei



Fonte: Statista ed elaborazioni Centro Studi TIM su dati Statista ed Eurostat. Tasso di cambio 0,84 sterline per 1 euro

L’OFFERTA - I

Polverizzazione

L’OFFERTA - I

Polverizzazione

Il settore della Cyber security in Italia: un mercato frammentato e iperspecializzato

La capacità di dotarsi di soluzioni efficaci e diffuse di cybersecurity da parte del sistema produttivo italiano presenta diverse criticità e ostacoli, tra cui una delle principali cause è la eccessiva frammentazione del mercato.

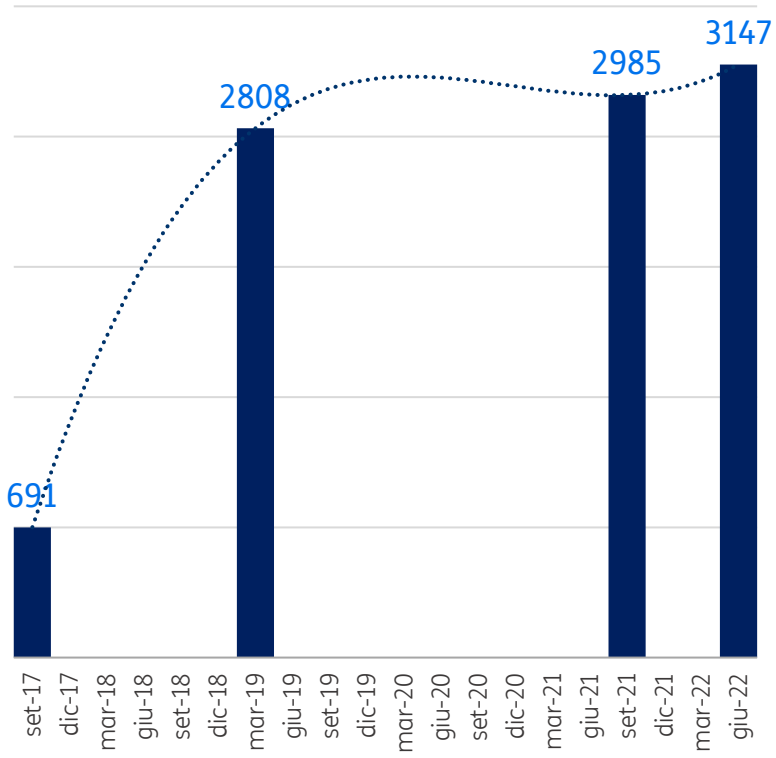
In molti casi, la nascita delle diverse realtà di piccola e media dimensione che oggi operano nel settore della cybersecurity italiana risulta riconducibile all’intuizione ed alle competenze di uno o più esperti che, sviluppando soluzioni ad hoc per far fronte a specifici problemi di sicurezza informatica, decidono di avviare una propria attività imprenditoriale. Il risultato di modelli di business e mission aziendali che, almeno inizialmente, sono molto puntuali e specializzati, ha portato ad un mercato in cui operano migliaia di aziende che offrono tecnologie e soluzioni software nella maggior parte dei casi non interoperabili e non integrabili tra di loro.

Questo modello è intrinsecamente connaturato alla realtà italiana. Anche in altri settori, la creatività individuale è stata il propellente principale per la costituzione di imprese che sono state capaci di affermarsi a livello nazionale ed internazionale. Tuttavia, in un settore caratterizzato da una continua trasformazione tecnologica, da economie di scala e di scopo e da una feroce concorrenza internazionale, affidarsi alla sola intuizione può rappresentare una forte criticità per la crescita e lo sviluppo delle aziende.

In Italia ci sono oltre 3100 imprese che dichiarano di offrire servizi di cybersecurity e/o di sicurezza informatica. Anche in questo caso, in modo speculare alla crescita di ricavi ed attacchi informatici, si tratta di un dato in forte crescita: le imprese che operavano in questo settore erano infatti meno di 700 nel 2017, mentre a metà del 2022 erano 3.147, un aumento di oltre 4 volte in cinque anni. La rilevazione è stata effettuata da Unioncamere-Infocamere sulla base dei dati del Registro delle imprese delle Camere di commercio.

Apparentemente la frammentazione del mercato si sta ulteriormente acuendo perché, se è vero che il giro d’affari del settore è cresciuto, non è però cresciuto a ritmi altrettanto vertiginosi. Negli ultimi 12 - 24 mesi si è assistito ad un parziale rallentamento, ma non ad un’inversione di tendenza.

Figura 7 – Le imprese di Cybersecurity in Italia



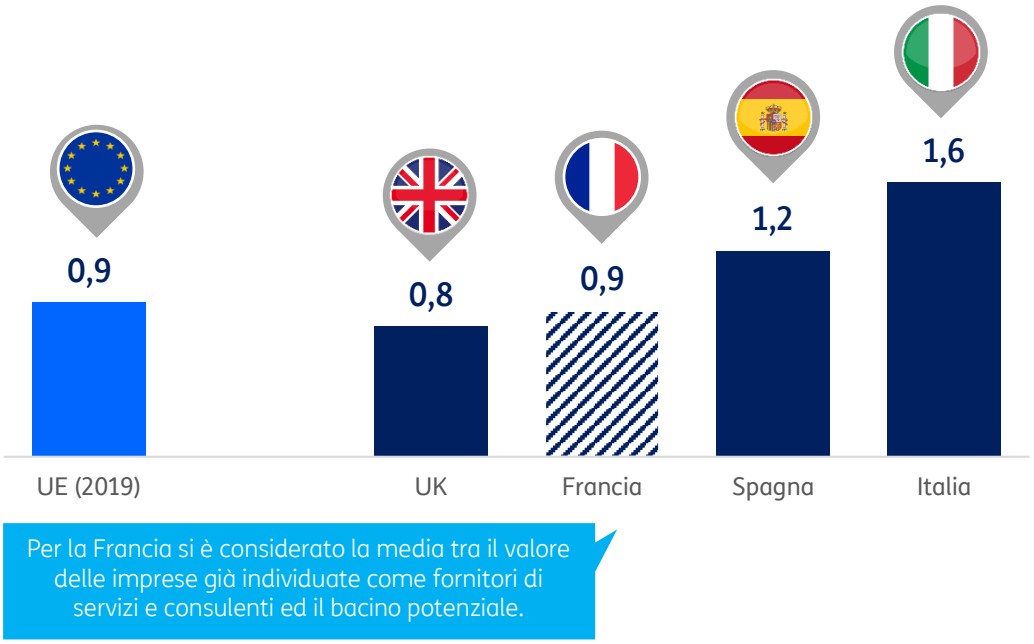
Fonte: Unioncamere-Infocamere e Movimprese. Indagine sulle imprese che dichiarano di occuparsi di attività di sicurezza IT / Cybersecurity. Vari anni

Per fissare un termine di paragone e meglio comprendere l'ipertrofia del contesto italiano basti pesare che nel 2019 in Europa si contavano quasi 0,9 imprese di cybersecurity per miliardo di PIL, mentre in Italia, nel 2022, ve ne sono 1,6 imprese ogni miliardo di PIL.

Certamente, anche in Europa si è assistito ad una proliferazione di imprese di cybersecurity analoga a quella che si è verificata in Italia al crescere delle minacce informatiche e pertanto questo confronto potrebbe apparire oggi superato. Tuttavia, il dato italiano appare significativamente più alto anche mettendolo a confronto con i settori della cybersecurity di Spagna e Regno Unito, che nel 2022 avevano censito, rispettivamente, all'incirca 1600 e 2000 imprese, ossia 1,2 e 0,8 imprese per miliardo di PIL. In pratica, il mercato italiano risulterebbe due volte più frammentato di quello inglese.

Per quanto riguarda la Francia, l'Agenzia per la Sicurezza Nazionale ANSSI ed il Ministero per l'Interno hanno costituito una piattaforma - Cybermalveillance.gouv.fr – ed in questo ambito si sta procedendo ad un censimento delle imprese che offrono servizi di cybersecurity in modo da avere una rappresentazione chiara e trasparente del sistema dell'offerta anche a vantaggio delle imprese clienti. Al momento sono state individuate circa 1450 imprese, distinte tra fornitori di servizi e consulenti, ma si ipotizza che il bacino di riferimento possa raccogliere circa 3000 aziende, portando il valore da 0,6 a 1,1 imprese per miliardo di PIL.

Figura 8 – Numero di imprese di Cybersecurity per miliardo di PIL



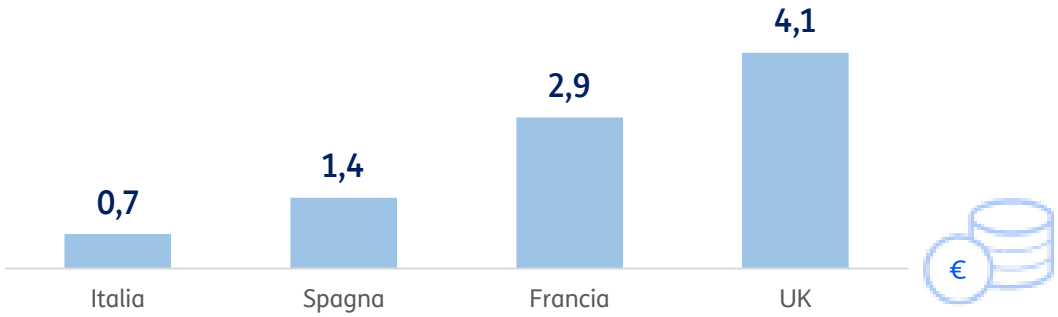
Fonte: elaborazione Centro Studi TIM su dati Unioncamere-Infocamere, INCIBE, Cybermalveillance.gouv.fr, Department for Digital, Culture, Media and Sport (DCMS), ECSO ed Eurostat. Per UK, tasso di cambio medio 2022 Banca d'Italia, pari a 0,853 sterline per un euro

Per completezza di informazione è opportuno osservare che il dato relativo all'Italia si riferisce ad imprese che nella descrizione delle proprie attività utilizzano le espressioni "sicurezza informatica" e/o "cyber security". Si tratta quindi di una rilevazione basata sulla capacità dichiarata dall'impresa di poter effettuare una determinata attività, magari in aggiunta ad altri servizi informatici che rappresentano il principale servizio offerto. È quindi possibile che il dato possa non essere immediatamente confrontabile e omogeneo con i valori indicati per la Spagna (rilevato dalla Agenzia Nazionale di Cybersecurity INCIBE) e del Regno Unito (in cui il valore è stato progressivamente filtrato per individuare le imprese effettivamente attive nel settore).

Fatta questa precisazione le informazioni raccolte e i diversi ordini di grandezza che emergono dal confronto ci permettono comunque di effettuare una serie di considerazioni che ci permettono di inquadrare e capire meglio come il settore della cybersecurity italiano si colloca rispetto a quello degli altri principali Paesi europei :

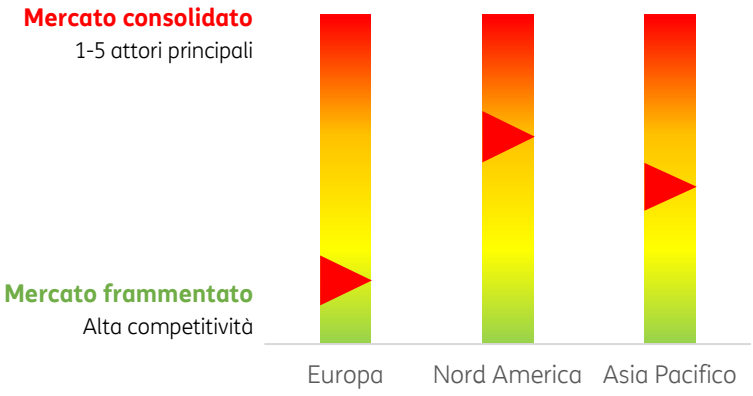
- **Dimensione delle imprese**. Come riportato in precedenza, il settore della cybersecurity italiano ha una dimensione di fatturato inferiore a quella di Francia e Regno Unito e un valore analogo a quello della Spagna. Dunque, anche a parità di imprese per miliardo di PIL, il fatturato medio per impresa in Italia risulterebbe comunque inferiore a quello degli altri contesti europei presi in esame. In effetti, rapportando il valore di fatturato stimato da Statista per il 2022 al numero di aziende di cybersecurity ne deriva che in Italia il valore dei ricavi medi per impresa è di circa 0,7 milioni di euro, in Spagna 1,3 milioni di euro, in Francia 2,9 milioni di euro e nel Regno Unito 4,1 milioni di euro.

Figura 8 – Ricavo medio per impresa (milioni di euro)



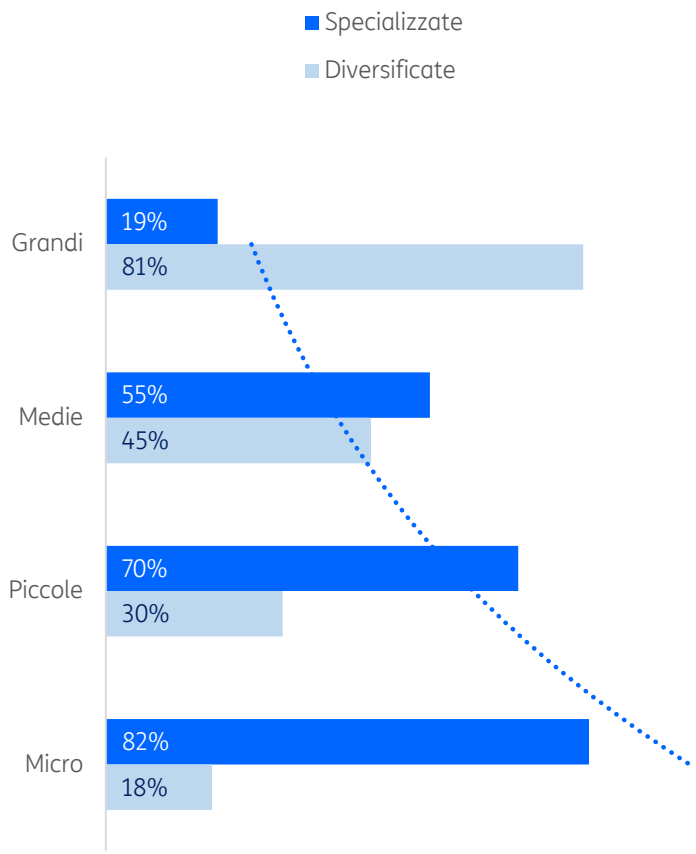
- **La frammentazione è una caratteristica che investe il settore della cybersecurity europea nel suo complesso**. Più in generale, per quanto l'Italia ne soffra in modo il particolarmente acuto, la frammentazione del settore della cybersecurity è un fattore che accomuna tutti i paesi europei, come è possibile desumere da diverse fonti. Ad esempio, confrontando i dati della società di ricerca Mordor Intelligence emerge che il settore della cybersecurity europeo è più frammentato di quelli del Nord America e dell'area Asia-Pacifico.

Figura 9 – Livello di concentrazione dei mercati della Cybersecurity nelle principali aree economiche mondiali



Fonte: riadattamento da Mordor Intelligence 2023

Figura 10 – Specializzazione nell'offerta di servizi di Cybersecurity per dimensione media di impresa



Fonte: Perspective Economics per DCMS

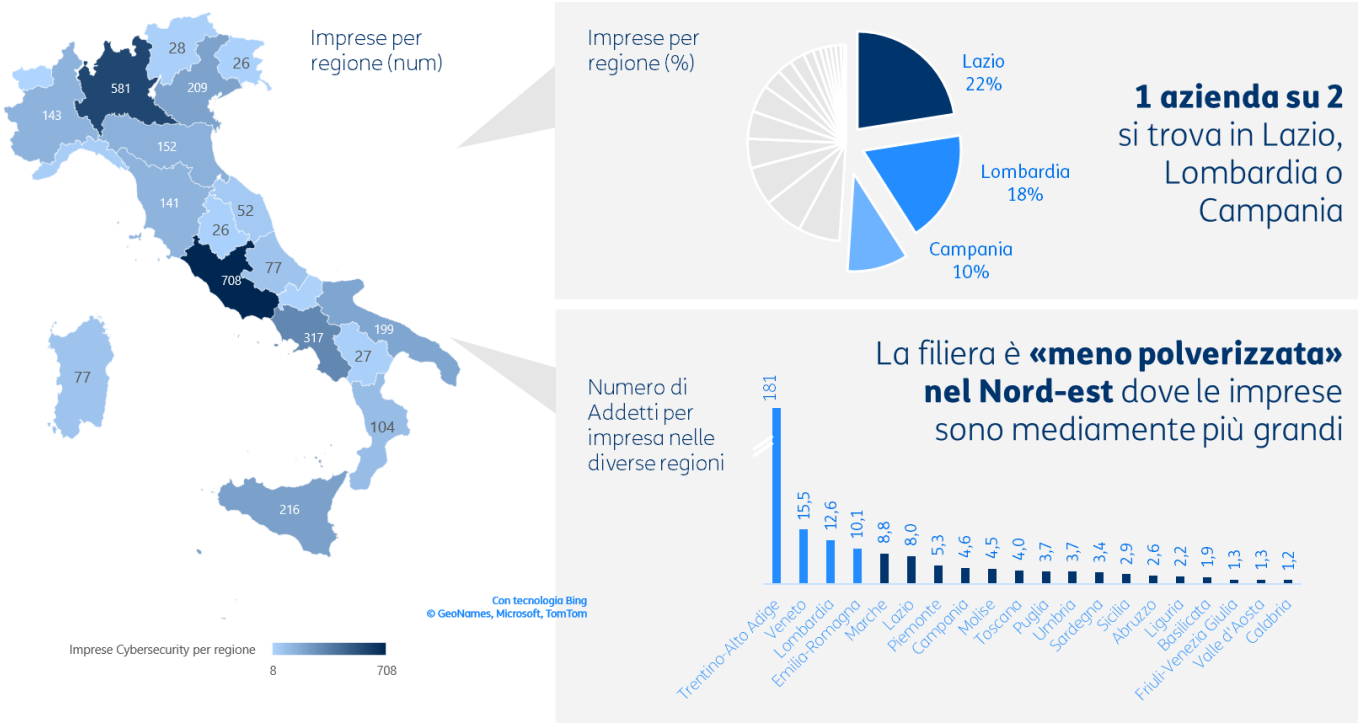
Il sottodimensionamento delle imprese ha degli effetti anche sull'ampiezza del portafoglio di offerta: più le imprese sono piccole e più si dedicano unicamente alla fornitura di servizi di cyber. (cosiddette imprese pure players) e, anche all'interno del campo cyber spesso si focalizzano sulla fornitura di unica tecnologia/soluzione che risponde ad una specifica necessità circoscritta.

Tale fenomeno emerge chiaramente osservando ad esempio la struttura del mercato inglese: tanto più grandi sono le aziende, tanto maggiore è la diversificazione dei servizi. Per 10 aziende di grande dimensione censite nell'insieme delle imprese di cybersecurity, solo 2 sono specializzate ed il rapporto si ribalta al diminuire della dimensione dell'impresa.

Aree di concentrazione e distretti industriali cyber

I dati dell'indagine Unioncamere-Infocamere mostrano che, nonostante la frammentazione del settore riguardi tutto il territorio nazionale, le imprese del Nord-est (Trentino-Alto Adige, Veneto, Lombardia ed Emilia-Romagna) sono mediamente di dimensioni maggiori rispetto al resto del Paese, probabilmente anche in virtù di una maggiore densità imprenditoriale e dinamismo dei rispettivi territori.

Figura 11 – Le imprese di Cybersecurity nelle regioni italiane

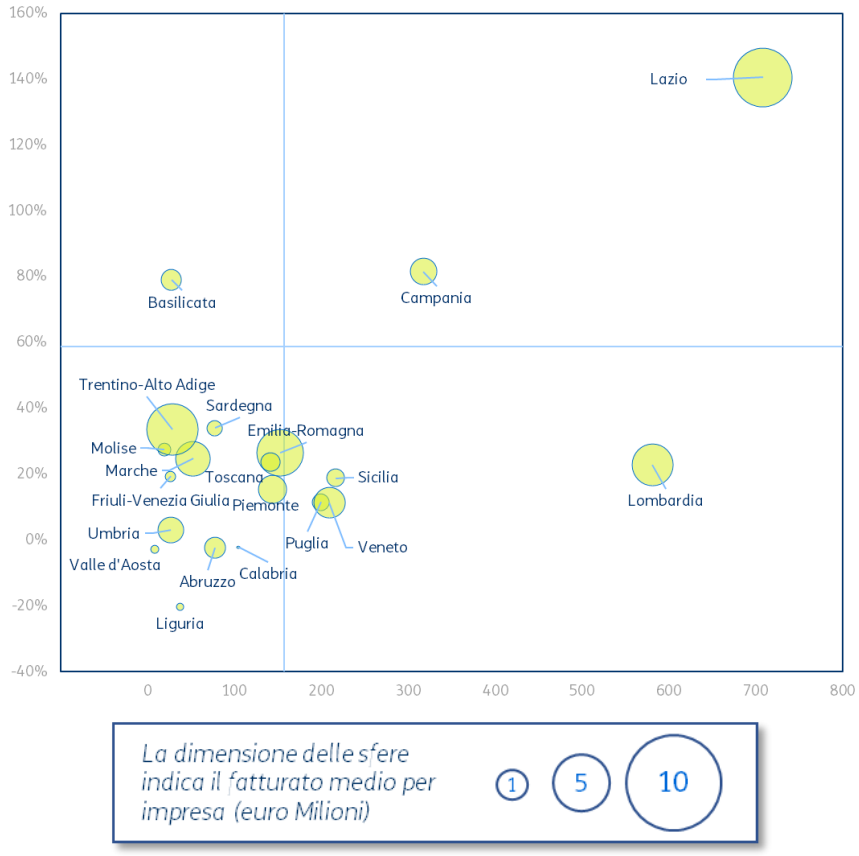


Fonte: elaborazione dati Unioncamere-Infocamere

In termini di presenza di imprese, i territori in cui si rilevano più aziende dedicate alla cybersecurity sono invece il Lazio, la Lombardia e la Campania in cui sono complessivamente presenti metà delle oltre 3.100 imprese registrate in Italia.

A livello di sviluppo del fatturato (che comunque aumenta con tassi di crescita a due cifre praticamente su tutto il territorio), a Lazio e Campania si aggiungono Basilicata e Trentino-Alto Adige. In quest'ultima area sembrano quindi presenti aziende mediamente più grandi in termini di addetti rispetto al resto del Paese e con un fatturato in forte crescita.

Figura 12 – Dimensioni e performance economiche delle imprese di Cybersecurity nelle regioni italiane



Fonte: elaborazione su dati Infocamere-Unioncamere

Questo dato è peraltro coerente con la presenza di "distretti tecnologici", come ad esempio a Roma, nella Tiburtina Valley dove si concentrano imprese del settore digitale e della difesa. In altri casi la densità di imprese cyber è stimolata dall'azione di soggetti pubblici o si amplifica grazie alle iniziative di istituti di ricerca ed università, come ad esempio in Trentino.

Promuovere la concentrazione di imprese tecnologiche in specifiche aree territoriali, in particolare nel settore della cybersecurity, è una prassi che si è riscontrata anche in altri Paesi, in cui si è seguito l'esempio del Cyberspark, il centro sulla cybersecurity israeliano nato nel 2014 a Be'er Sheva e diventato oggi il baricentro di un ecosistema sulla sicurezza informatica tra i più sviluppati, che ha reso Israele il secondo esportatore di tecnologie cyber al mondo. La creazione di questo hub che raccoglie start-up, imprese più affermate, centri di ricerca universitari e istituti di formazione civili e della difesa, è stato in grado di attrarre l'attenzione di venture capitalist globali, alimentando la

crescita di diverse società promettenti che si sono trasformate in quelli che vengono definiti “unicorn”.

Anche in Francia, nel 2022, è stato inaugurato il Campus Cyber di Parigi, una partnership pubblico-privata, tra lo stato francese e i grandi attori che sostengono il progetto, tra cui Airbus, Orange, Capgemini, Atos, Thales. Il progetto verrà replicato a livello territoriale: sono stati lanciati analoghi centri in Nouvelle-Aquitaine (Pessac) e Hauts-de-France (Lille). Altre aree di attrazione delle imprese di cybersecurity sono a Rennes, dove sono già presenti diversi incubatori digitali a cui se ne aggiungerà uno interamente dedicato alla cybersecurity (Cyber Place), a Tolosa dove è presente il Campus della Cyberdefence di Orange.

In Germania una delle maggiori concentrazioni di imprese di cybersecurity interessa la regione North Rhine-Westphalia, in particolare a Bochum, mentre in Spagna, dove è molto sviluppata la filiera della cybersecurity nell’area dei Paesi Baschi, si sta lavorando per costituire un polo di attrazione per le imprese del settore sfruttando la presenza del Centro delle Nazioni Unite per le tecnologie dell'informazione e della comunicazione (UNICTF).

L’OFFERTA - II

Evoluzione

L'OFFERTA - II

Evoluzione

L'evoluzione delle società di cybersecurity quotate

Analizzando la struttura dell'offerta dl mercato cyber possiamo concettualmente dividere le aziende in tre grandi gruppi.

I grandi protagonisti del settore ICT italiano, gruppi di grandi dimensioni che presentano una gamma di offerta ampia ed articolata e nella quale trovano spazio anche prodotti e servizi di cybersecurity. Raramente tale offerta è basata su soluzioni proprietarie, ossia sviluppate in-house. È più comune il caso in cui si sviluppano alcuni prodotti in-house e – grazie alle competenze, alle certificazioni accumulate, al personale specializzato – si può fornire ai clienti una suite completa utilizzando le soluzioni dei grandi fornitori internazionali di prodotti di cybersecurity.

Le imprese specializzate nell'offerta di servizi cyber, tipicamente di media dimensione, che grazie a soluzioni specifiche e mirate ed a investimenti finalizzati a irrobustire la propria offerta, hanno saputo costruire delle posizioni di forza e di riconoscibilità nel settore. Alcune di queste aziende, che potremo definire "*Pure Cybersecurity Players*", hanno intrapreso il percorso della quotazione in Borsa al fine di sostenere l'evoluzione verso una scala dimensionale che possa garantire loro una certa indipendenza. Tra le imprese quotate troviamo anche Gruppi ICT di media dimensione con una propria azienda dedicata alla cybersecurity che potremo annoverare nel gruppo dei Pure Players.

I medi e piccoli fornitori di servizi iperspecializzati, che rappresentano la maggior parte delle imprese del settore, prevalentemente realtà mirate e focalizzate su specifici prodotti-soluzioni e "poco strutturate" che rappresentano in pieno ancora oggi il "modus operandi" prevalente del settore.

Il modello di evoluzione del settore: focus sulle medie aziende quotate

Per quanto si tratti di un contesto ad alta crescita, le società di cybersecurity che si sono quotate in borsa sono poco più di una decina e congiuntamente rappresentano circa il 13%-15% dell'intero fatturato del settore. Queste società, per quanto in numero limitato, rappresentano la miglior proxy di quello che potrebbe essere il percorso evolutivo e/o il punto di arrivo per quelle società che riescono a compiere il necessario salto dimensionale.

Lo "scale up", inteso non tanto come passaggio da start-up a impresa con business plan più consolidati, ma come ampliamento dimensionale di una certa entità che permette di sfruttare le importanti economie di scala e scopo da cui è caratterizzano il settore, appare infatti un passaggio obbligato per tutte quelle imprese che vogliono darsi una prospettiva di lungo periodo.

Proprio al fine di meglio comprendere il modello di evoluzione del settore più verosimile, il Centro Studi TIM ha condotto un'analisi prendendo in esame un campione di circa venti imprese, che include tutte le aziende quotate e alcune tra le medie aziende più dinamiche. Le aziende quotate, anche in virtù dell'importante disclosure di informazioni a cui sono tenute ci ha permesso di esaminare e valutare i singoli portafogli di offerta, le strategie di crescita nonché gli asset e le tecnologie distintive.

Le principali evidenze che emergono dall'analisi condotta sono le seguenti:

- **Prevale il modello "one stop shop"**. Più della metà delle società analizzate hanno portafogli di offerta ampi, che coprono la maggior parte dei servizi di cybersecurity che vengono proposti sul mercato. Raggruppando i prodotti ed i servizi offerti in 7 cluster principali (in particolare: Governance & Compliance, Attività di Monitoraggio, Difesa & Investigazione, Raccolta Dati relativi ad Eventi, Analisi delle Vulnerabilità, Analisi delle Minacce, Formazione), il 75% delle imprese esaminate offre servizi di Difesa e Investigazione. Più in generale, stanno emergendo come elementi fondamentali del portafoglio di offerta la fornitura di un servizio di SOC (Security Operations Center) a cui si aggiungono servizi di verifica delle vulnerabilità (Penetration Test) e analisi delle minacce (Open Source Intelligence). Se ne può dedurre che questi siano anche i servizi più richiesti sul mercato.

Figura 13 – Servizi di Cybersecurity offerti dalle imprese del campione esaminato

Fonte: analisi Centro Studi TIM

- **Nel 75% dei casi le aziende hanno almeno un prodotto proprietario**. I 3/4 delle società esaminate possiede almeno un prodotto proprietario, che rappresenta quindi un elemento chiaro e distintivo con cui le aziende possono proporsi sul mercato, integrando in caso l'offerta con soluzioni fornite dai grandi provider internazionali di servizi. Più in generale, nel 40% dei casi la soluzione offerta è basata su una tecnologia sviluppata in house.

- **Società cyber specializzate si rivolgono a imprese che operano in specifici ambiti ICT**. Le società che con portafoglio di offerta più ristretto tipicamente si specializzano nel presidio di uno specifico segmento di clientela verticale, ossia offrono soluzioni mirate ad uno specifico campo di attività, come ad esempio protezione dei sistemi cloud, IoT, ecc.

Da questa panoramica, si può dedurre che il salto dimensionale, nella maggior parte dei casi, può avvenire seguendo due percorsi, il primo dei quali si basa sul combinato disposto di una gamma di offerta che copre a 360 gradi tutte le funzioni chiave della cybersecurity e uno o più prodotti di punta proprietari, che rappresentano un biglietto da visita sul mercato e sono in grado di attrarre clienti. Il secondo percorso si basa invece sullo sviluppo di un'offerta mirata a coprire le necessità di una specifica tipologia di clienti.

Le imprese piccole ed "iperspecializzate" ed i fornitori ICT generalisti

I casi appena osservati, in cui le imprese nate da un'idea originale riescono a strutturarsi in modo da intraprendere un percorso di crescita che può sfociare anche nella quotazione in Borsa, rappresentano una minoranza nell'insieme delle 3.100 aziende che costituiscono il bacino di riferimento del settore.

Al modello di vendita diretta di propri prodotti e soluzioni da parte di "Pure Cybersecurity Players" si affianca un secondo modello che potremmo definire di "Non Pure Cybersecurity Players" basate sulla vendita indiretta di soluzioni non sviluppati al proprio interno. In questi casi, in cui gli operatori sono prevalentemente distributori di servizi di grandi società globali, si assiste anche al fenomeno di "cattura" (acquisizione) di piccole società iperspecializzate, estremamente verticali su uno specifico segmento o in possesso di tecnologie promettenti, attraverso cui i Non Pure Cybersecurity Players possono proporsi sul mercato con soluzioni originali e proprietarie, come ben evidenziato nello schema seguente.

Figura 14 – Imprese di Cybersecurity specializzate e non specializzate

Fonte: adattato da Pwc da Mordor Intelligence (2021) – Global cybersecurity market – Growth, trends, COVID19 impact

In questo modo, è possibile fornire un modello di offerta integrata che risponde pienamente alle esigenze delle piccole e medie imprese italiane che, come vedremo nel prossimo capitolo, preferiscono acquisire una suite più o meno completa di servizi di cybersecurity (che ad esempio contempli al proprio interno sia servizi di compliance alla normativa, sia formazione per i dipendenti sia soluzioni software per rilevare e rispondere ad attacchi infornatici, ecc.) da un unico soggetto.

LA DOMANDA

Esternalizzazione

LA DOMANDA

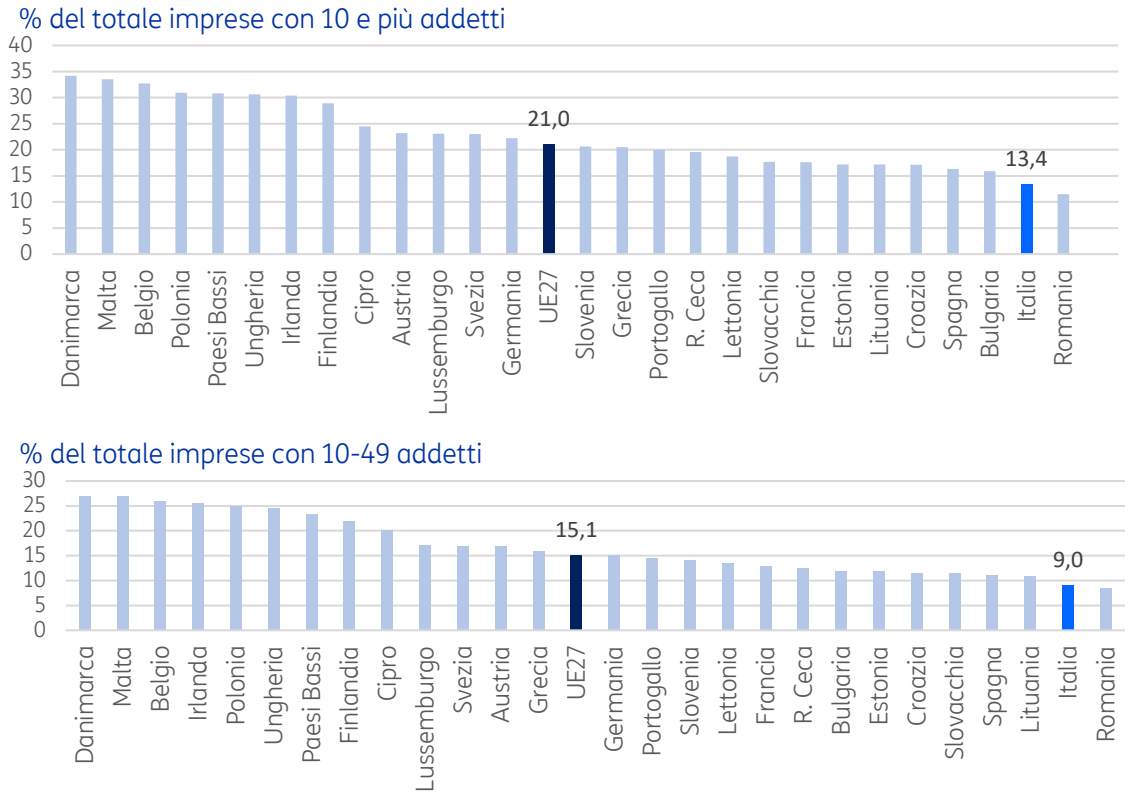
Esternalizzazione

le PMI preferiscono esternalizzare

Come noto ed ampiamente documentato il sistema economico e produttivo italiano è caratterizzato in larghissima parte dalla presenza di piccole e medie imprese, elemento che si è rivelato spesso un punto di forza in termini di dinamicità, inventiva ed imprenditorialità diffusa, ma che altrettanto spesso si è rivelato un fattore di debolezza.

Per quanto riguarda la presenza di specialisti e addetti ICT, anche a parità del fattore dimensionale (ovvero considerando imprese delle medesime dimensioni) ciò che si riscontra confrontando le imprese italiane con quelle degli altri paesi europei è una minore tendenza, che è quasi un'assenza, tra le piccole medie imprese ad assumere e dotarsi di persone con competenze cyber al proprio interno. Secondo i dati Eurostat, tra le imprese italiane sopra i 10 addetti solo un'impresa su dieci può vantare all'interno del proprio organico personale con competenze ICT.

Figura 15 – Imprese che assumono specialisti ICT per dimensione media di impresa

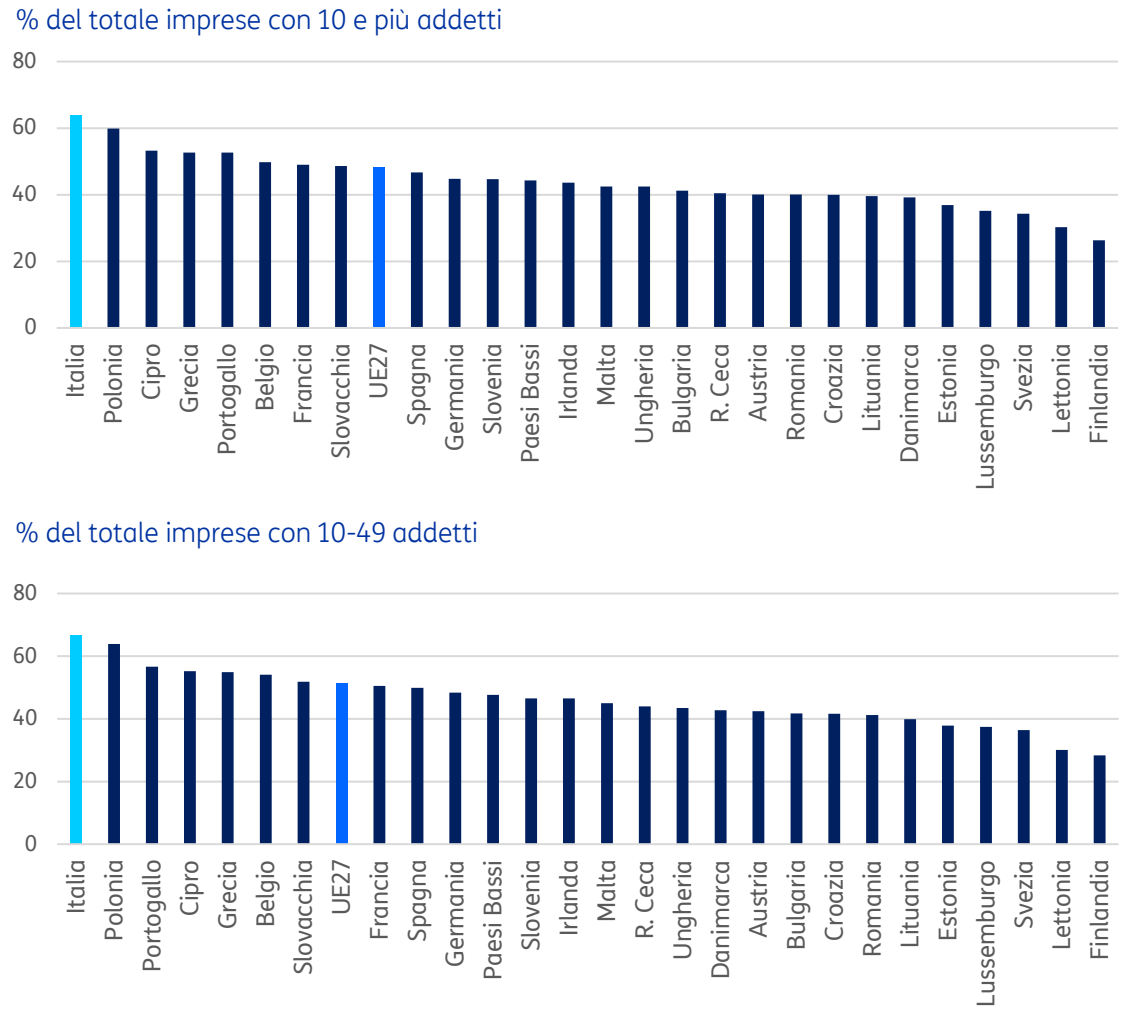


Fonte: Eurostat

La domanda di mercato: le PMI e la scelta del fornitore/modalità di fornitura dei servizi di cyber security

Come logica e naturale conseguenza di questa pressoché totale assenza di competenze ICT al proprio interno, le imprese italiane e, nello specifico quelle che decidono di dotarsi difese contro possibili attacchi cyber, lo fanno necessariamente affidandosi interamente a soggetti esterni: le imprese italiane nella maggior parte dei casi (più di 6 su 10 imprese) ricorrono a personale esterno: non avendo competenze ICT al proprio interno non si hanno neanche competenze in tema di cybersecurity. Il dato del ricorso all'outsourcing è ancora più alto restringendo l'osservazione alle imprese 10-49 addetti (quasi 7 aziende su 10).

Figura 16 – Esternalizzazione delle attività di Cybersecurity per dimensione media di impresa



Fonte: elaborazioni Centro Studi TIM su dati Eurostat

Questo aspetto, se da un certo punto di vista può offrire una prospettiva interessante per le società fornitrici di servizi ICT (e di cybersecurity), da un altro lato ostacola una reale e effettiva comprensione dei rischi sottostanti e, come vedremo, complica e rende più difficile il matching tra domanda e offerta legata a causa di una forte asimmetria informativa nella ricerca e contrattualizzazione del giusto partner-fornitore.

La domanda di mercato: le PMI e la scelta del fornitore/modalità di fornitura dei servizi di cyber security

L'assenza di personale con competenze ICT, oltre ad avere come inevitabile conseguenza l'esternalizzazione di qualsiasi attività di cyber security, si ripercuote necessariamente sulla scelta del fornitore e sulla modalità di contrattualizzazione del medesimo. Mentre le imprese che vantano specialisti ICT o personale dedicato a gestire gli aspetti della sicurezza informatica hanno necessità di ricorrere a società specializzate esterne per rispondere alla complessità delle minacce informatiche, ma sono consapevoli delle funzionalità dei sistemi e sono in grado di gestire in autonomia le fasi di "normale amministrazione", le PMI che risultano prive di qualsivoglia competenza informatica, sono costrette ad affidarsi interamente alle competenze e al "metro di giudizio" del loro fornitore.

Proprio a causa dell'assenza di risorse ICT nel proprio organico, nel momento in cui le PMI italiane affrontano l'esigenza di dotarsi sistemi e soluzioni di protezioni da attacchi cibernetici nella maggioranza dei casi, lo fanno con "poca cognizione di causa" e "poca convinzione" e spesso senza saper esattamente di che cosa hanno bisogno. Sono invece consapevoli dei danni che ne possono derivare e sono probabilmente disposte a spendere per mitigare il rischio cyber senza però arrivare ad impiegare risorse interne dedicate, che dal punto di vista di una piccola e media impresa viene vissuto come uno "spreco" o comunque come una sottrazione di risorse all'attività di produzione e commercializzazione.

Le PMI preferiscono rivolgersi alle grandi imprese ICT

Ulteriore conseguenza della forte asimmetria informativa, ossia della scarsa capacità di valutare e comprendere a fondo la "bontà" e "l'adeguatezza" delle soluzioni che loro vengono offerte, le PMI tendono a rivolgersi a soggetti che già conoscono e di cui ci si fidano maggiormente. I grandi fornitori ICT sono ritenuti più affidabili anche in ragione di un contratto già in essere che può essere esteso ad altri ambiti di servizio, integrando l'offerta di servizi di cybersecurity all'interno nel pacchetto di soluzioni già messe a disposizione dell'azienda cliente.

Essenzialmente si tratta di una questione di "trust" e, tipicamente, le grandi imprese, in virtù della loro lunga storia, della loro dimensione e della maggiore solidità, ispirano maggiore fiducia anche perché sono ritenute in grado di garantire una maggiore continuità temporale rispetto ad altri soggetti più piccoli, peraltro attivi in un mercato meno noto ed estremamente dinamico, in cui non è infrequente il passaggio di mano (con un possibile adeguamento delle policy di offerta) se non il fallimento. Al contrario, dal punto di vista di una PMI, la grande impresa c'è oggi e ci sarà anche domani.

Infine, c'è da considerare che le PMI tendono a rivolgersi alle grandi aziende anche perché, non sapendo spesso di cosa hanno bisogno nell'ambito della sicurezza informatica, hanno la consapevolezza che un grande fornitore "generalista" è in grado di offrire più o meno qualsiasi servizio necessario.

La figura del broker/system integrator

In effetti, per facilitare ulteriormente lo sviluppo del mercato, c'è bisogno non tanto o non solo di fornitori di servizi cyber affidabili, quanto di consulenti in grado di assistere le imprese indicando quali siano i servizi necessari, eventualmente fornendoli in prima persona. Spesso l'incontro tra le PMI ed i fornitori di cybersecurity avviene a seguito di un incidente informatico, oppure per la necessità di rispettare degli obblighi legati alla gestione di dati e informazioni o il bisogno di certificazioni (ad esempio, la ISO 27001). In altri casi sono le associazioni industriali di categoria che promuovono incontri tra domanda ed offerta a scopo informativo e formativo. Si tratta quasi sempre di situazioni episodiche e incontri quasi casuali, mentre al contrario la definizione di un sistema di sicurezza informatica richiede una strategia ed una progettazione che seguono una visione chiara delle esigenze e degli strumenti che possono essere messi in campo, di una condivisione di obiettivi tra fornitore e cliente che possa rafforzarsi nel corso del tempo per far crescere allo stesso tempo la consapevolezza dei rischi e la fiducia nelle tecniche di mitigazione che l'azienda di cybersecurity scelta sia in grado di mettere in campo.

In questo quadro, emerge con insistenza la necessità di un broker, di un system integrator che possa consigliare le PMI, seguendone la loro evoluzione passo dopo passo e che al tempo stesso si riveli capace di mettere assieme i diversi pezzi del mosaico che permettano loro di mitigare i rischi derivanti dagli attacchi cibernetici.

In fondo, per fare un parallelo con uno degli aspetti più tipici della vita quotidiana, le esigenze delle PMI non sono molto distanti da quelle che ciascuno di noi sperimenta quando ha bisogno di assistenza medica. Nella maggior parte dei casi, è raro che ci si rivolga direttamente ad un medico specialista (cardiologo, endocrinologo ecc.). È più facile fissare prima un appuntamento con il proprio medico di base che, sulla base delle conoscenze pregresse e le informazioni acquisite durante la visita, è in grado di indirizzare il proprio paziente verso lo specialista più adeguato.

Alle PMI in realtà serve qualcuno che, oltre svolgere contemporaneamente il ruolo di medico di base e di medico specialista, sia anche in grado di fornire e somministrare le cure necessarie (farmacia e servizi ospedalieri).

LA CYBERSECURITY MADE IN ITALY CHALLENGE

Collaborazione

LA CYBERSECURITY MADE IN ITALY CHALLENGE

Collaborazione

Il rischio di disallineamento tra domanda e offerta

Purtroppo, l'esigenza tipica delle PMI di poter contare su offerte "a 360 gradi" non si concilia bene con una struttura dell'offerta dei servizi di cybersecurity, a tutt'oggi caratterizzata da una forte frammentazione e da un alto livello di focalizzazione su singoli servizi/prestazioni. La maggior parte della miriade di imprese che operano in questo settore, nate per dare risposte puntuali a problemi specifici, non rappresenta il migliore fornitore possibile. Per riprendere l'analogia precedente, l'impresa cyber di piccole dimensioni e focalizzata su una singola prestazione/nicchia del comparto cyber nella maggior parte dei casi non è in grado di fornire allo stesso tempo "diagnosi, prognosi e terapia".

Se i piccoli fornitori di cybersecurity non rappresentano una risposta completa, i fornitori medio-grandi di soluzioni ICT non sono specializzati nella sicurezza informatica e superano questa criticità o offrendo soluzioni chiavi in mano di grandi player internazionali di cybersecurity oppure, acquisendo piccole realtà cyber ed integrandone i loro servizi all'interno del proprio portafoglio d'offerta. Se da un lato questo "allargamento del portafoglio di offerta per incorporazione", rappresenta una risposta alle esigenze delle PMI, dall'altro impedisce la crescita autonoma delle piccole realtà italiane che non riescono a compiere l'auspicato salto dimensionale e vengono assorbite e inglobate all'interno di realtà più grandi, dove spesso si perde, o comunque scema, lo spirito innovatore e imprenditoriale.

Occorre pertanto una visione nuova, un modello di sviluppo alternativo che, affiancandosi alle strategie appena viste, possa essere in grado di promuovere la crescita delle realtà di cybersecurity più promettenti, senza doverne necessariamente compromettere l'indipendenza e la crescita autonoma, rafforzando la base di un settore che è nel tempo diventato uno dei più strategici per le economie avanzate.

Una Cybersecurity "Made in Italy"

Un'ulteriore conferma dell'importanza crescente del settore e della necessità di operare per rafforzare le imprese e consolidare la struttura della filiera può essere trovata nelle diverse iniziative che sono state portate avanti recentemente in alcuni Paesi europei, seguendo l'onda della costituzione di una "Cybersecurity Made in Europe". L'iniziativa, lanciata dallo European Cyber

Security Organization ha lo scopo di promuovere le società europee di sicurezza informatica e aumentare la loro visibilità sul mercato europeo e globale attraverso un "bollino di qualità" che possa porsi come marchio di garanzia ed affidabilità per i clienti finali. In Italia, molte aziende hanno ottenuto il sigillo, erogato dal Comitato Nazionale per la Ricerca in Cybersecurity (a cui partecipano l'Istituto di informatica e telematica del CNR, il Consorzio interuniversitario nazionale per l'informatica CINI, e il Consorzio nazionale interuniversitario per le telecomunicazioni CNIT).

In modo speculare, tale iniziativa è stata replicata anche a livello di singoli paesi membri come ad esempio "IT Security Made in Germany" in Germania e "Cyber Expert" per la Francia. Indipendentemente dalla forma e dai modelli di funzionamento adottati rispettivamente dalle istituzioni europee, tedesche e francesi, le iniziative citate hanno come obiettivo comune quello di promuovere le imprese domestiche certificandone la qualità, il pieno rispetto delle normative europee e attestandone la provenienza geografica (paese in cui sono state sviluppate le soluzioni software vendute). Ad esempio per poter ottenere il marchio "IT security Made in Germany" le imprese tedesche devono soddisfare le seguenti condizioni: 1) l'headquarter della società deve essere in Germania; 2) le soluzioni offerte devono essere "affidabili"; 3) nei prodotti offerti dalla società non devono esserci "accessi nascosti" (no backdoors); 4) la ricerca e sviluppo delle soluzioni di cyber security devono avvenire in Germania; 5) la società deve rispettare le leggi e le normative sulla privacy e sulla protezione dei dati personali in vigore in Germania.

In buona sostanza, si tratta cioè di mettere a disposizione delle imprese un marchio di qualità ("bollino blu") ovvero una sorta di denominazione di origine controllata e garantita come quella che tipicamente si trova sui vini. Mentre l'intento dichiarato è quello di promuovere e rafforzare un settore e una filiera chiave che non può e non deve essere interamente delegata a paesi di altre aree geografiche.

Per l'Europa è fondamentale che i paesi membri giochino un ruolo da protagonisti nella costruzione e consolidamento di un mercato di soggetti di cyber security saldamente ancorati ai valori e ai principi costituenti dell'Unione Europea. Questo rappresenta lo spirito che ha guidato la nostra iniziativa di promozione del settore di cybersecurity, tanto più importante per il nostro Paese, dove il richiamo al "Made in Italy" rappresenta molto più di una semplice "label".

Perché una Cybersecurity Made in Italy Challenge: Matching tra domanda - offerta e modello a scaffale

Lo scopo della "Cybersecurity Made in Italy Challenge" è quello di consolidare la crescita delle piccole realtà fondate in Italia e in Europa che vantano prodotti all'avanguardia tecnologica e che, tuttavia, sono ancora tutt'oggi alla ricerca di un solido percorso di crescita organica. In altri termini, questa iniziativa ha l'obiettivo di facilitare l'incontro tra le imprese Pure Cybersecurity soprattutto

italiane, che dispongono di soluzioni e competenze ultra-specialistiche, e le esigenze ed i bisogni espressi e manifestati più o meno consapevolmente dalle PMI italiane. Un anello di congiunzione tra domanda ed offerta che sia in grado di completare il panorama dell'ecosistema della cybersecurity.

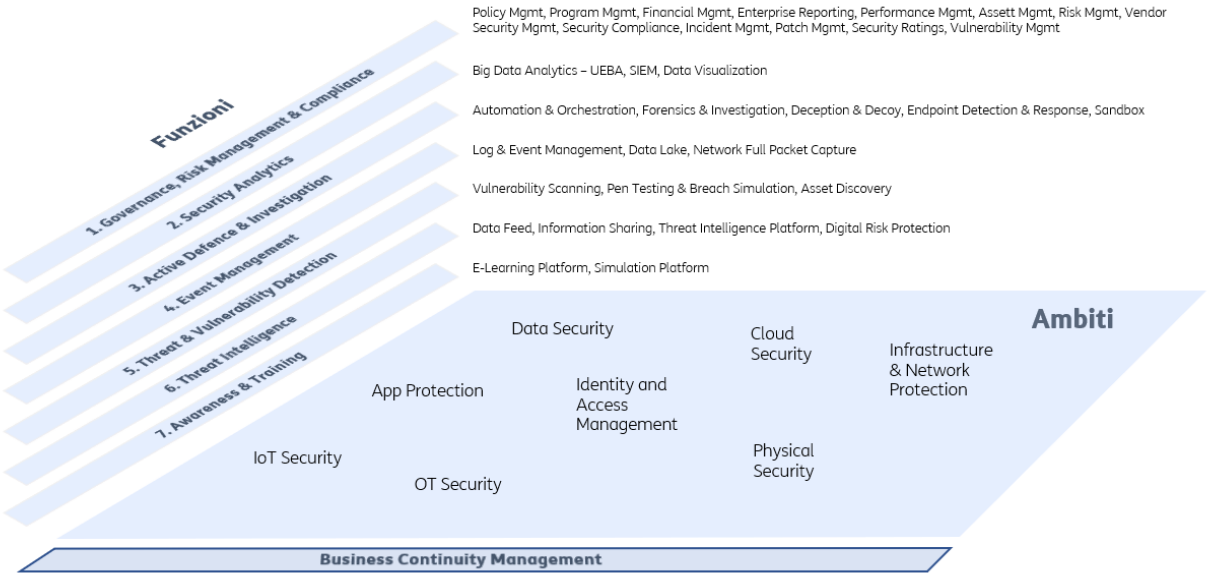
Il contributo che si è voluto fornire con Cybersecurity Made in Italy Challenge è offrire un'alternativa sia al modello di crescita autonoma e indipendente (che riesce a pochi), sia alla cessione delle attività a soggetti di maggiori dimensioni. Con questa iniziativa TIM intende dare la possibilità alle tante imprese della galassia della cybersecurity italiana di farsi conoscere e acquisire nuovi clienti preservando la propria identità e autonomia. Per raggiungere questo obiettivo TIM mette a disposizione la propria visibilità e reputazione e i propri canali di vendita per costruire un rapporto tra pari e costruire benefici e vantaggi reciproci.

La Cybersecurity Made in Italy Challenge ricalca, nella sua struttura e nella sua formula, altre iniziative di Open Innovation che il gruppo TIM ha intrapreso sia in Italia (ad esempio, la Piattaforma TIM Growth) sia – prima ancora - in Brasile, "aprendo un canale" di conoscenza reciproca che possa dare risalto a molte realtà innovative e di talento.

La condivisione e "apertura" degli asset del Gruppo a realtà esterne rappresenta in altri termini un modello che sempre di più sarà sviluppato in maniera continuativa e strutturata anche in un'ottica di andare ad alimentare lo sviluppo dei servizi che possono essere offerti attraverso le reti 5G, che offrono nuove e interessanti opportunità di crescita B2B e richiedono la costruzione di solide partnership con attori di altri settori (dalla mobilità alla manifattura, dalla salute ai servizi finanziari). Maggiore è la possibilità di creare connessioni, anche inusuali, all'interno degli ecosistemi che costituiscono il settore digitale italiano, maggiore è la possibilità di far crescere tutta la filiera e accelerare la digitalizzazione e l'innovazione del Paese.

NOTA METODOLOGICA

Di seguito si evidenzia la mappa di classificazione dei servizi utilizzata per valutare la gamma di offerta proposta sul mercato dalle società sopra elencate.



Limiti di responsabilità

I dati e le informazioni cui si fa riferimento nel presente documento sono forniti in buona fede e TIM le ritiene accurate. In nessun caso TIM sarà ritenuta responsabile per qualsiasi danno diretto o indiretto, causato dall'utilizzo di queste informazioni. I dati, le ricerche, le opinioni o i punti di vista espressi da TIM S.p.A non rappresentano dati di fatto. I materiali contenuti in questo documento riflettono le informazioni e le opinioni alla data di pubblicazione originale. Le informazioni e le opinioni espresse in questo documento sono soggette a modifiche senza preavviso. TIM non ha alcun obbligo o responsabilità di aggiornare i materiali di questa pubblicazione di conseguenza. TIM non sarà, in nessuna circostanza, responsabile per qualsiasi investimento, decisione commerciale o di altro tipo basata o presa in base ai contenuti di questo documento.

Si ringraziano Statista e Osservatorio Cybersecurity & Data Protection della School of Management del Politecnico di Milano per i dati forniti.

CENTRO STUDI

TIM