AGENDA DIGITALE – 4 APRILE 2025

Competenze per la cybersicurezza: la chiave per proteggere il Paese

di Alessandro D'Amato e Domenico Salerno

Il rapporto annuale dell'Osservatorio I-Com sulla Cybersicurezza analizza il panorama della cybersecurity nazionale. Focus su formazione, compliance aziendale e sviluppo di competenze digitali per contrastare le minacce

La **minaccia cibernetica ha assunto un ruolo sempre più centrale tra le sfide nazionali, eurounitarie e globali** affrontate dalle istituzioni, soprattutto in virtù dell'instabilità geopolitica degli ultimi anni che influenza il panorama della cybersicurezza.

Difatti, **siamo dinanzi ad attacchi sempre più gravi**, numerosi e specializzati, che spingono i Paesi e le organizzazioni internazionali allo sviluppo di policy, strategie e normative che pongono al centro la tutela del cyberspazio per cittadini, imprese e articolazioni statali.

L'ultimo ultimo rapporto annuale dell'Osservatorio I-Com sulla Cybersicurezza

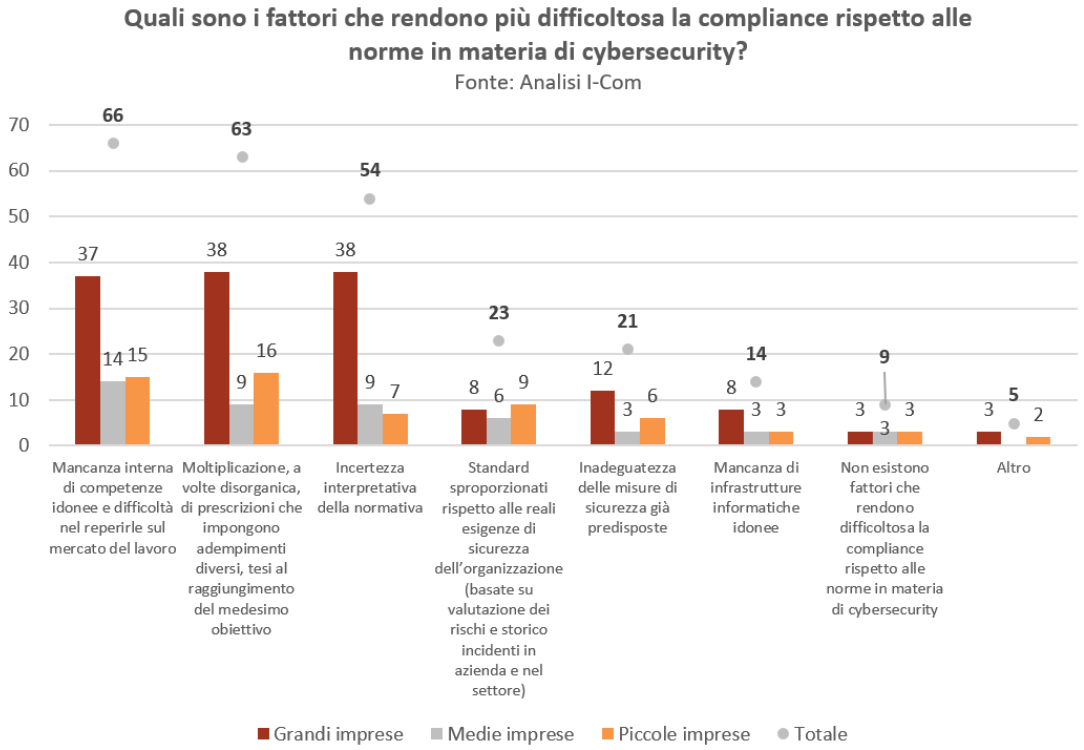
L'ultimo ultimo rapporto annuale dell'Osservatorio I-Com sulla Cibersicurezza prova a fare chiarezza su questo complessissimo quadro, mettendo in fila tutte le principali questioni aperte che riguardano l'ecosistema italiano della cybersicurezza. In particolare, il documento, dal titolo "**Competitività alla prova della cybersecurity. La sicurezza informatica in Italia e in Europa tra innovazione e regole**", approfondisce sia le problematiche relative alla compliance, sia le fragilità strutturali a livello nazionale, provando a restituire una fedele istantanea dello stato della sicurezza informatica nel nostro Paese.

La survey I-COM

Tra gli aspetti più interessanti indagati da I-Com all'interno dello studio sopra menzionato si evidenzia particolarmente quello della **preparazione delle imprese in ambito cybersicurezza**. Più nel dettaglio, al fine di verificare la rispondenza applicativa del quadro regolatorio europeo e nazionale in materia di cybersecurity, I-Com ha riproposto e aggiornato un'indagine avviata a partire dallo scorso anno, avvalendosi anche del sostegno di alcune delle principali associazioni di categoria, che in questa edizione ha coinvolto 150 imprese appartenenti a vari settori: utilities (acqua, rifiuti ed energia), trasporti, TLC/digitale, ecc.

Innanzitutto, **ai soggetti partecipanti è stato chiesto di fornire una valutazione circa l'impatto degli adempimenti prescritti dalle normative in cybersicurezza** sulla competitività aziendale. Per le grandi imprese rilevano maggiormente gli investimenti tecnico-organizzativi necessari alla compliance, così come per le aziende di medie dimensioni e per le piccole imprese. Considerando unitamente tutte le classi dimensionali, altri due motivi ricorrenti si rivedono nella preoccupazione circa l'innalzamento delle barriere all'ingresso, soprattutto per le PMI e la numerosità degli oneri burocratici e amministrativi richiesti.

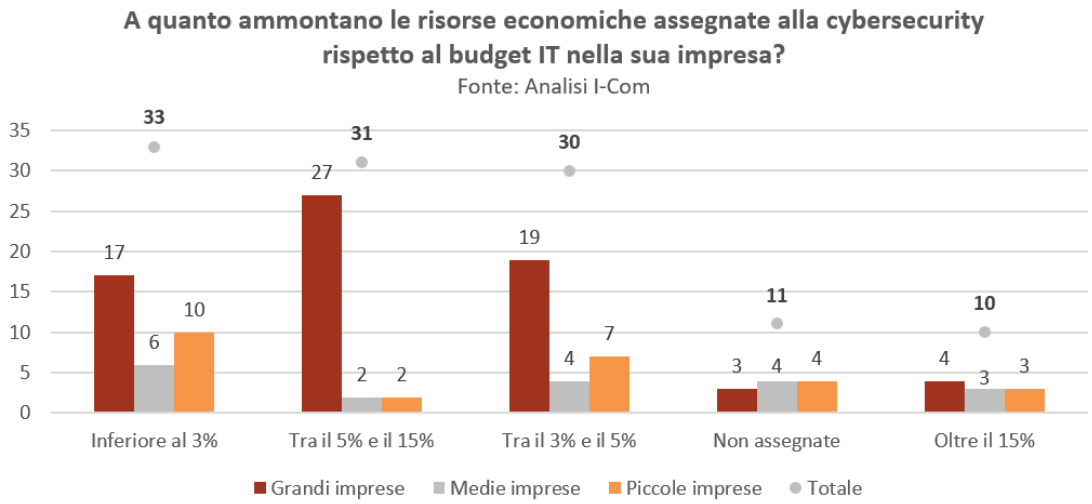
Successivamente, è stato chiesto alle imprese intervistate di **indicare nello specifico i fattori che rendono più difficoltosa la compliance rispetto alle norme in materia di cybersecurity** ed è emerso che ciò sarebbe dovuto alla mancanza di competenze idonee sia internamente, sia sul mercato del lavoro (66 risposte in totale), seguito dalla moltiplicazione – a volte disorganica – di prescrizioni che impongono adempimenti diversi, ma che sono tese al raggiungimento del medesimo obiettivo (63 risposte) e dall'incertezza interpretativa della normativa (54 risposte).



Gli investimenti delle imprese in ottica NIS 2

Il miglioramento del livello di sicurezza informatica, in ambito aziendale e non solo, passa inevitabilmente anche dal volume di risorse investite per raggiungere tale scopo. A questo riguardo, i dati emersi dall'indagine I-Com sono allarmanti, in quanto la maggioranza delle imprese assegna meno del 3% del budget IT alla cybersecurity. Considerando l'aggravarsi dello scenario, sia in termini numerici che di impatto, circa le attività malevole a danno delle infrastrutture critiche anche in Italia, nonché dei maggiori adempimenti previsti – fra le altre – dalla **direttiva NIS2**, è stato chiesto alle aziende partecipanti di fornire indicazioni su un eventuale incremento delle risorse destinate alla cybersecurity.

Sul punto, si può osservare come il 42,11% delle imprese stia ancora valutando tale eventualità (il 9% in meno rispetto al 2023), mentre solo il 25,44% ha già deciso di aumentare gli investimenti in cybersicurezza, facendo registrare un sostanziale peggioramento su base annua (-11%).



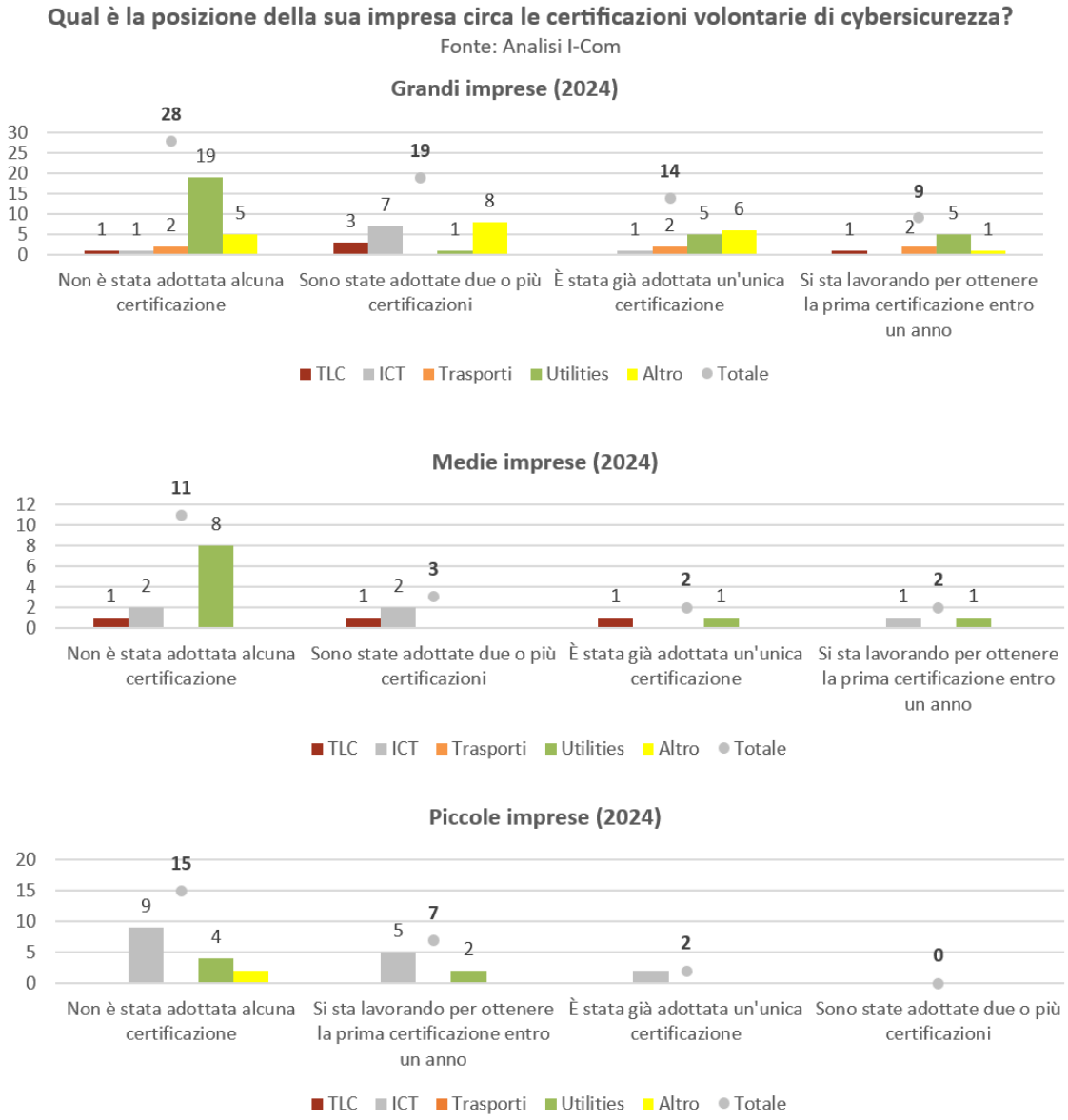
Il tema delle certificazioni

Un ruolo importante nel migliorare la sicurezza e la resilienza degli ecosistemi informatici delle imprese è riconosciuto in capo all'**adozione delle certificazioni di cybersicurezza**. Queste ultime infatti spingono l'azienda a migliorare le proprie capacità di risposta al rischio e a far emergere le vulnerabilità prima che possano essere sfruttate dai cybercriminali.

Analizzando **i dati raccolti da I-Com rispetto alle certificazioni volontarie** di cybersicurezza, si può osservare che gran parte delle imprese delle tre classi dimensionali non ha conseguito alcun tipo di certificazione. Tuttavia, emergono segnali moderatamente positivi se si confrontano i dati su base annua. Difatti, mentre nell'edizione 2023 coloro che dichiaravano ciò corrispondevano a oltre il 63%, nell'ultima rilevazione sono scesi al 48%. Tra questi, le piccole imprese sono quelle che hanno performato meglio rispetto all'anno scorso (-23,2%), seguite dalle grandi (-15,5%) e, infine, dalle medie (-13%).

Tali risultati trovano una motivazione negli **ostacoli che sono percepiti dalle imprese con riguardo all'ottenimento di una certificazione di questo tipo**. Similmente a quanto osservato per il 2023, il principale intralcio risiede nei costi elevati del processo di certificazione, che non sono percepiti come proporzionati ai benefici che ne possono conseguire (il 34,8%). In secondo luogo, quasi il 19% sostiene che i tempi per l'esecuzione della valutazione e il rilascio della certificazione sono troppo lunghi. In

terzo luogo, il 14,5% ritiene che la necessità di ripetere la procedura di valutazione in caso di nuove patch per aggiornamenti sia uno degli aspetti che limitano il perseguimento di una certificazione di cybersicurezza.



Fonte: Analisi I-Com

Tra coloro che hanno dichiarato di aver adottato almeno una certificazione, i principali effetti positivi direttamente riconducibili ad essa sono stati: un **miglioramento dell'immagine e della reputazione dell'impresa** nei confronti degli stakeholders (46,3%), una maggiore consapevolezza dei dipendenti e dei collaboratori esterni (39%) e più possibilità di partecipare a bandi di gara pubblici o privati (28%).

Inoltre, il 74,5% delle aziende è parzialmente o totalmente d'accordo in merito al fatto che standard comunitari – come gli **European Common Criteria-based cybersecurity certification scheme (EUCC)** – possono incentivare il ricorso alle certificazioni (+4,5% rispetto al 2023). Posto che il 31 gennaio 2024 la Commissione europea ha adottato il Regolamento di esecuzione 2024/482 (*Implementing Act*) con cui gli EUCC sono diventati ufficialmente parte della legislazione europea, nell'ultima edizione dell'indagine è stato chiesto di rendere noto il punto di vista della propria organizzazione circa l'eventualità di un approccio mandatorio o meno sull'adozione di schemi di certificazioni europei come, appunto, gli EUCC. Ebbene, oltre il 70% dei rispondenti ha dichiarato che non si è ancora assunta una posizione sul tema. Pertanto, la restante quota di imprese si divide tra chi ha optato per un approccio volontario (15,6%) e chi per quello mandatorio (12,8%).

Il nodo competenze in materia di cybersicurezza

Come è sottolineato chiaramente anche dalla survey realizzata da I-Com, la formazione degli individui riveste un ruolo fondamentale nell'ambito della cybersicurezza. Nel merito, l'Italia è più indietro rispetto alla media dei Paesi europei e presenta una diffusione di competenze digitali altamente variegata a seconda della fascia d'età. Ad esempio, le competenze digitali almeno di base sono diffuse in una quota pari al 45,8% della popolazione italiana, a fronte di un 55,6% a livello UE. Un dato interessante emerge a proposito della consapevolezza sui pericoli digitali, infatti, rispetto agli individui che non utilizzano l'Internet of Things per timori legati alla sicurezza, l'Italia presenta quote sensibilmente più basse rispetto alla media UE. Ciò detto, nel corso del 2024 si è riscontrato un significativo incremento degli illeciti legati al fenomeno delle truffe online nel nostro Paese. Difatti, secondo gli ultimi dati della Polizia Postale sono aumentati sia i casi trattati che le somme di denaro sottratte.

Nell'ambito della **formazione ICT delle imprese**, il nostro Paese è nuovamente al di sotto della media europea. Addirittura, la quota di imprese ICT con più di 10 addetti che erogano formazione al proprio personale è diminuita negli ultimi anni, dal 19,4% del 2019 al 17,9% del 2024. Allo stesso tempo, sempre in Italia, **il costo medio delle violazioni di dati è aumentato maggiormente rispetto a Germania e Francia**, passando da 3,9 milioni di dollari nel 2021 a 4,7 nel 2024. Tutti questi elementi

segnalano una situazione allarmante per la formazione e la consapevolezza sui rischi digitali in Italia, per cui risulta necessario investire su iniziative idonee a formare i cittadini, affinché acquisiscano al meglio queste capacità, indipendentemente dal livello di alfabetizzazione digitale già in loro possesso.

Il monitoraggio I-Com sulla formazione cyber

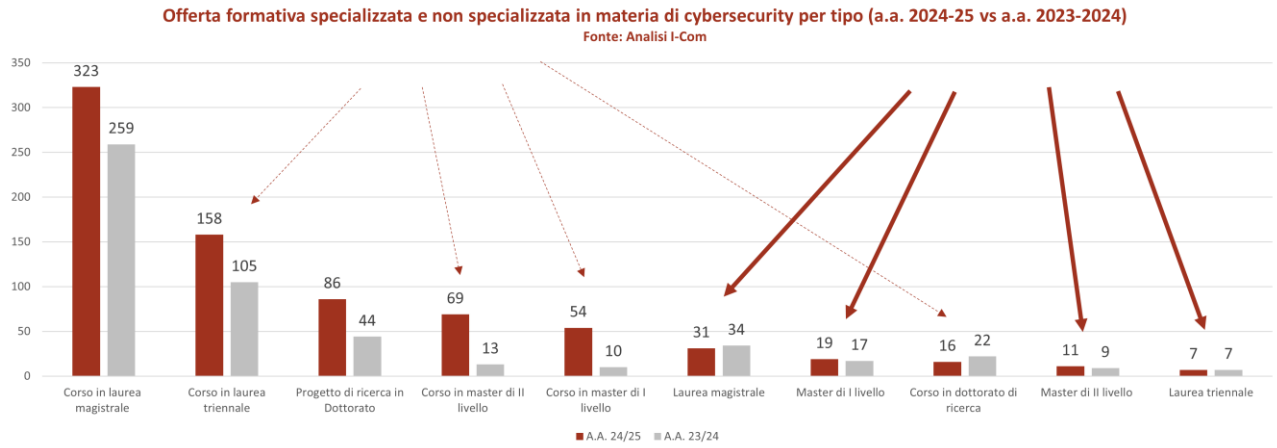
Il miglioramento del livello di **competenze in cybersicurezza**, sia nella popolazione generale che sul mercato del lavoro, passa inevitabilmente dal potenziamento dell'offerta formativa in quest'ambito. Per comprendere se gli enti che erogano istruzione superiore in Italia stanno adeguando i propri programmi alle necessità del Paese, I-Com ha avviato da due anni un monitoraggio periodico dell'offerta formativa in cybersicurezza in Italia.

L'ultima versione dell'analisi, aggiornata all'anno accademico 2024/2025, presenta 774 tra corsi e insegnamenti relativi alla cybersicurezza, il che segnala un netto miglioramento rispetto ai 520 individuati a inizio 2024 (+48% su base annua).

Nel dettaglio, l'analisi ha individuato **323 insegnamenti singoli all'interno di corsi di laurea magistrale**, 158 insegnamenti singoli all'interno delle lauree triennali, 86 progetti di ricerca in dottorati, 69 corsi singoli in master di II livello e 54 in master di I livello, a fronte di 31 lauree magistrali, 30 master, 16 corsi all'interno di dottorati di ricerca, 11 corsi singoli all'interno di master di I e II livello e **7 lauree triennali** interamente dedicate alla cybersecurity. Pertanto, il totale delle lauree specifiche (triennali e magistrali) sul tema della cybersicurezza ammonta a 38. La formazione post-laurea si affianca a quella universitaria con differenze in termini quantitativi piuttosto importanti: tra progetti di ricerca in dottorati e master di primo e secondo livello sono stati conteggiati ben 116 corsi "specializzati", ben 46 in più rispetto a quelli individuati a inizio 2024. Nel complesso, la formazione specializzata in materia di cybersicurezza in Italia ha raggiunto quota 154 corsi di studio interamente dedicati, segnando un incremento pari al 38,7% su base annua. Per quanto riguarda la distribuzione regionale della complessiva offerta formativa, questa appare piuttosto disomogenea con una forte concentrazione nel Lazio (180 tra corsi e singoli insegnamenti), in Lombardia (119) e in Campania (70).

Tuttavia, se si considerano i dati normalizzati per il numero di Università presenti sul territorio regionale, **la classifica varia** mostrando in prima posizione il Piemonte con un rapporto 13,5:1, seguito da Liguria (13:1) e Puglia (12,8:1). A livello regionale, a gennaio 2025 solo Basilicata e Valle d'Aosta risultavano non proporre corsi di questo genere. In relazione alla distribuzione regionale della offerta formativa "specializzata" (lauree triennali, magistrali, master e progetti di ricerca in dottorati), il Lazio si conferma la regione più interessata con 32 percorsi complessivi, catalizzando ben 5 lauree dedicate, oltre a 12 progetti di ricerca in dottorato e 15 master. In questo contesto, non sorprende che oltre il 60% dell'offerta formativa universitaria in materia di cybersicurezza risulti erogata dai dipartimenti di ingegneria (48,1%) e informatica (16,8%). Inoltre, l'elevato numero di master specifici sui temi della cybersicurezza (30) sembra suggerire un'elevata domanda di approfondimento post-laurea su questi temi.

Nell'ambito della **formazione superiore,** un ruolo di rilievo è rivestito certamente dagli ITS che hanno lo scopo di formare personale tecnico in aree strategiche per lo sviluppo del tessuto economico del Paese, tra cui spiccano l'area 6 "Tecnologie della informazione e della comunicazione". Il portale online curato dall'Istituto Nazionale Documentazione Innovazione Ricerca Educativa (INDIRE) evidenzia che sul territorio nazionale sono presenti 147 ITS. Come si evince dal monitoraggio INDIRE e da un'analisi svolta da I-Com, gli ITS che si occupano di cybersicurezza sono il 35,4% rispetto al numero complessivo di quelli attivi, una quota più che raddoppiata rispetto alla rilevazione precedente effettuata a inizio 2024. In particolare, l'offerta formativa erogata ha visto l'avvio di un numero considerevole di corsi in sicurezza informatica specifici e di singoli insegnamenti sul tema all'interno di corsi attinenti a materie differenti.



Conclusioni

In definitiva, analizzando quanto emerge dal rapporto I-Com, si può affermare che la cybersicurezza ad oggi rappresenti sempre più un elemento imprescindibile nei processi decisionali delle imprese. Queste ultime si muovono in un panorama costituito da minacce e strumenti per combatterle, di natura legislativa oltre che tecnica, per cui al fine di affrontare al meglio le nuove sfide del cyberspazio appare necessario puntare sull'aumento delle competenze e della consapevolezza, senza sottovalutare l'importanza dell'istaurazione di un continuo dialogo partecipato tra privati e istituzioni, affinché le prassi e le prescrizioni normative non diventino un ostacolo, ma un ombrello protettivo per i destinatari delle stesse.

Il tema delle competenze e della consapevolezza appare quanto mai complesso con riferimento al contesto nazionale. Ed infatti, i dati citati rivelano una grave arretratezza da parte dell'Italia in materia di competenze e consapevolezza digitali.

Sulla scorta di queste premesse, appare cruciale insistere sul rafforzamento della cultura di base in cybersicurezza, dato che le tecniche e le modalità degli attacchi cibernetici che singoli individui e organizzazioni pubbliche e private subiscono ancora oggi e che si ripercuotono in maniera anche piuttosto importante sulle rispettive attività quotidiane sono pressoché le medesime ormai da diversi anni. Pertanto, è necessario investire su iniziative idonee a formare i cittadini, affinché acquisiscano al meglio queste capacità, indipendentemente dal livello di alfabetizzazione digitale già in loro possesso. Inoltre, non andrebbe sottovalutato il valore della formazione continua, digitale e specializzata in cybersecurity per le imprese, soprattutto se di micro e piccole dimensioni, anche in virtù del fatto che a breve saranno pienamente applicabili

importanti normative dell'UE connesse a tale materia, il che comporterà nuove sfide per i soggetti che ricadono nel rispettivo campo di applicazione.

Anche nell'ottica di estendere il più possibile la formazione specialistica nell'ambito della cybersicurezza, assumono particolare rilevanza gli Istituti Tecnici Superiori (ITS), i quali possono fungere da ulteriore e fondamentale anello di congiunzione tra la realtà scolastica e quella lavorativa. Attualmente, la formazione garantita dai 147 ITS attivi sul territorio, seppur in aumento, non pare sufficiente a colmare il gap di personale specializzato in questo campo. Di conseguenza, un aumento più consistente di questo tipo di Istituti e, in particolare, l'incremento degli ITS in ambito ICT (Area 6), nonché di quelli che si occupano di tematiche connesse alla cybersicurezza (corrispondenti al 35,4% rispetto al numero complessivo di quelli attivi) potrebbe costituire un ulteriore tassello in direzione della costruzione e del rafforzamento di un ecosistema maggiormente resiliente di fronte alle crescenti minacce provenienti dalla rete, anche in virtù dell'instabile scenario geopolitico attuale.