BANCA D'ITALIA
EUROSISTEMA

Mercati, infrastrutture, sistemi di pagamento

(Markets, Infrastructures, Payment Systems)

Indagine conoscitiva sul mercato italiano dei servizi di testing di cybersicurezza

di Anna Barcheri, Luca Bastianelli, Tommaso Curcio, Luca De Angelis, Paolo De Joannon, Gianluca Ralli e Diego Ruggeri

Settembre 2025

Numero 63

BANCA D'ITALIA
EUROSISTEMA

Mercati, infrastrutture, sistemi di pagamento

(Markets, Infrastructures, Payment Systems)

Indagine conoscitiva sul mercato italiano dei servizi di testing di cybersicurezza

di Anna Barcheri, Luca Bastianelli, Tommaso Curcio, Luca De Angelis, Paolo De Joannon, Gianluca Ralli e Diego Ruggeri

Numero 63 – Settembre 2025

I lavori pubblicati nella collana "Mercati, infrastrutture, sistemi di pagamento" presentano documentazioni e studi su aspetti rilevanti per i compiti istituzionali della Banca d'Italia in tema di monitoraggio dei mercati finanziari e del sistema dei pagamenti, nonché di sviluppo e gestione delle relative infrastrutture. L'intento è quello di contribuire alla diffusione della conoscenza su questi argomenti e di favorire il dibattito tra le istituzioni, gli operatori economici, i cittadini.

I lavori pubblicati riflettono le opinioni degli autori, senza impegnare la responsabilità dell'Istituto.

La serie è disponibile online sul sito www.bancaditalia.it.

Copie a stampa possono essere richieste alla casella della Biblioteca Paolo Baffi: richieste.pubblicazioni@bancaditalia.it.

ISSN 2724-6418 (online)
ISSN 2724-640X (stampa)

Banca d'Italia
Via Nazionale, 91 - 00184 Roma - Italia
+39 06 47921

Grafica e stampa a cura della Divisione Editoria e stampa della Banca d'Italia

INDAGINE CONOSCITIVA SUL MERCATO ITALIANO DEI SERVIZI DI TESTING DI CYBERSICUREZZA

di Anna Barcheri*, Luca Bastianelli*, Tommaso Curcio*, Luca De Angelis*, Paolo De Joannon, Gianluca Ralli***, Diego Ruggeri*****

Sintesi

Autorità e operatori sono da tempo impegnati nel rafforzare la cybersicurezza dell'intero settore finanziario. Il recente regolamento europeo sulla resilienza operativa digitale (DORA) introduce regole armonizzate tra cui l'obbligatorietà, per alcune istituzioni finanziarie, di svolgere i test avanzati di cybersicurezza – cc.dd. *Threat-Led Penetration Testing* (TLPT). L'indagine si propone di analizzare l'offerta di tali servizi in Italia, individuando la dimensione del settore e approfondendo la struttura del mercato. Attraverso un questionario su base volontaria, sono state valutate le caratteristiche dell'offerta tra cui i volumi, i fattori abilitanti e gli ostacoli allo sviluppo del settore. L'indagine ha evidenziato un mercato dinamico e in espansione, con una prevalenza di operatori italiani. L'erogazione dei servizi TLPT è concentrata. Emerge una forte variabilità nell'impiego delle risorse, evidenziando un'offerta non ancora standardizzata: l'adozione di framework di riferimento coesiste ancora con l'impiego di metodologie proprietarie. Tra gli ostacoli principali allo sviluppo del mercato emergono la carenza di personale qualificato e i costi che si mantengono a livelli elevati.

Classificazione JEL: G28, K24, L11, L86

Parole chiave: Cybersecurity, Cybersecurity services, Cyber resilience, Cyber risk, DORA, Financial sector, Market Analysis, Red Teaming, Testing, Third party provider, Threat Intelligence, TIBER-EU, TIBER-IT, TLPT.

Abstract

Authorities and market participants have long been committed to strengthening the cybersecurity of the entire financial sector. The recent EU regulation on digital operational resilience (DORA) has introduced harmonized rules, including the requirement for certain financial institutions to conduct advanced cybersecurity tests – known as Threat-Led Penetration Testing (TLPT).
This paper analyses the supply of TLPT services in Italy, assessing the sector's size and examining the structure of the market. Based on a voluntary-response questionnaire, we evaluate the key characteristics of the supply side, including service volumes, enabling factors, and barriers to the sector's development. The findings point to a dynamic and growing market, with a predominance of domestic providers. TLPT service provision is concentrated in the hands of a small number of players, and there is significant variability in the resources allocated to individual services, indicating a market offering that is not yet fully standardized. Regulatory frameworks coexist with proprietary methodologies. Among the main obstacles to market development are a shortage of skilled professionals and persistently high costs.

* Banca d'Italia, Dipartimento Pagamenti e infrastrutture di mercato.

** Banca d'Italia, Dipartimento Pagamenti e infrastrutture di mercato, fino a marzo 2025; al momento BCE, unità Euro Digitale.

*** Banca d'Italia, Dipartimento Vigilanza bancaria e finanziaria.

INDICE

1. PREMESSA[1]

La digitalizzazione del sistema finanziario, lo sviluppo di modelli di offerta e di fruizione *online* dei servizi agli utenti e la crescente complessità della catena di fornitura accrescono l'esposizione ai rischi informatici, inclusi quelli di natura cibernetica. Il settore finanziario è un obiettivo privilegiato degli attori della minaccia cyber per vari fattori strutturali: la rete di interconnessioni, il predominante contenuto tecnologico, la profittabilità degli attacchi e la crescente velocità delle transazioni di mercato e delle operazioni di pagamento che lo caratterizzano (FMI, 2024).

Tra gli strumenti che le entità finanziarie possono adottare per innalzare le capacità di difesa figurano i test avanzati di cybersicurezza di tipo *Threat-Led Penetration Testing* (TLPT). Nel 2018 il G7 ha definito il TLPT come un tentativo controllato di compromettere la resilienza cibernetica di un operatore simulando le tattiche, le tecniche e le procedure di attori della minaccia reali (G7, 2018). Il TLPT si basa su due fasi principali: la raccolta di informazioni mirate e utili sull'entità testata, conosciuta come "*Targeted Threat Intelligence*" e il "tentativo di compromissione", noto anche come "*red teaming*"[2].

Il TLPT riveste un'importanza crescente anche per le autorità ai fini della salvaguardia della stabilità, efficienza e continuità di servizio del sistema finanziario, nel suo complesso e a livello delle singole istituzioni vigilate. La Banca Centrale Europea (2018) ha definito una metodologia standardizzata per i test di tipo TLPT, il *Framework for Threat Intelligence-Based Ethical Red Teaming* (TIBER-EU), recentemente aggiornata[3]. Essa è stata implementata in Italia congiuntamente dalla Banca d'Italia, dalla Consob e dall'Ivass nel 2022 con la metodologia TIBER-IT, che consente di svolgere i test su base volontaria. Dal 17 gennaio 2025 è applicabile il Regolamento UE 2022/2554 sulla resilienza operativa digitale (DORA), che prevede l'obbligatorietà di questa tipologia di test per alcuni operatori critici identificati secondo dei criteri quali-quantitativi.

Tra i requisiti del TIBER-EU vi è l'uso obbligatorio di fornitori esterni per i servizi di *Threat Intelligence* (TI), mentre ne è fortemente consigliato l'uso per i servizi di *Red Teaming* (RT)[4]. Tali servizi, soprattutto quelli di *red teaming*, sono oggetto di particolare attenzione, considerato che comportano l'accesso a dati e informazioni confidenziali e sensibili del soggetto che si sottopone al test e che hanno un ruolo fondamentale nell'esecuzione del test stesso. Sebbene il TIBER-EU stabilisca delle linee guida per i fornitori, attualmente non esistono schemi di accreditamento. Inoltre, non vi è una conoscenza approfondita del livello di maturità dell'offerta di servizi TLPT, data la scarsità di dati e analisi relativi a questo mercato.

L'indagine qui presentata intende approfondire la struttura del mercato italiano dei servizi di cybersicurezza, con particolare riferimento a due tipologie di servizi per il testing, quelli per la *threat intelligence* e per il *red teaming*. L'indagine, su base volontaria, è stata rivolta alle imprese del settore con sede in Italia che offrono i servizi in esame.

Dopo avere riassunto i principali risultati del lavoro (§2), si descrivono le attività di testing, il contesto normativo e ricerche di mercato nell'ambito della cybersecurity (§3). Successivamente si

[1] Si ringraziano Claudio Impenna, Giuseppe Grande, Caterina Beccarini e Antonino Fazio per il supporto e le revisioni accurate e puntuali, nonché i colleghi del Settore Supervisione outsourcer e terze parti per gli utili commenti forniti; Barbara Massalin e Wojciech Zamiar per i loro significativi contribuiti alla realizzazione del questionario nelle prime fasi di questo lavoro. Un ringraziamento speciale va a Marco Bottone per i suoi preziosi consigli dal punto di vista statistico e metodologico.

[2] Il *red teaming* è un concetto noto da tempo nel settore militare e in altri fortemente focalizzati sulla sicurezza. Solo più recentemente è stato introdotto nel mondo della cybersicurezza, dove le pratiche più consolidate erano rappresentate dalle attività di *penetration test* e *vulnerability assessment*. Nel campo della cybersicurezza del settore finanziario il *red teaming* guidato dalla valutazione delle minacce si è diffuso con l'introduzione dello schema CBEST da parte della Banca d'Inghilterra nel 2013. Questo è stato seguito da framework concettualmente comparabili in altre giurisdizioni, come l'iCAST a Hong Kong (2016) e infine dal TIBER, avviato nei Paesi Bassi e formalizzato in ambito Eurosistema con il TIBER-EU (2018).

[3] L'aggiornamento, di febbraio 2025, ha incorporato le lezioni apprese durante i vari test e si è reso necessario per il completo allineamento alle norme tecniche di regolamentazione contenute in DORA. Cfr. comunicato della BCE: https://www.ecb.europa.eu/press/intro/news/html/ecb.mipnews250211.en.html.

[4] In via eccezionale è possibile utilizzare tester interni.

riportano, con un progressivo livello di dettaglio, i risultati dell'indagine suddivisi in: caratteristiche delle imprese individuate e dei rispondenti (§4); caratteristiche dell'offerta dei servizi di cybersicurezza, con riferimento specifico a quelli di testing (§5); analisi di dettaglio sull'offerta dei servizi di TLPT (§6). L'ultimo capitolo contiene delle considerazioni conclusive (§7). Infine, tre appendici presentano una nota metodologica, una descrizione della struttura e delle domande principali del questionario utilizzato e un glossario di alcuni dei termini tecnici utilizzati.

2. PRINCIPALI RISULTATI

L'indagine è stata somministrata a 180 società con sede legale in Italia che offrono servizi di testing di cybersicurezza o affini. A causa dell'assenza di un codice ATECO[5] specifico per i servizi di cybersicurezza, queste società sono state individuate utilizzando varie fonti informative (con la metodologia descritta nell'Appendice A). La popolazione presa a riferimento si distribuisce in modo pressoché omogeneo tra le varie categorie dimensionali (le microimprese sono 42, le piccole 43, le medie 52 e le grandi 43). Hanno risposto 71 delle 180 società, con un tasso di risposta del 39,4 per cento. Tra le distribuzioni della popolazione e quelle dei rispondenti non si sono rilevate differenze significative in termini di classe dimensionale, macroarea geografica e anzianità societaria.

Caratteristiche delle imprese. – La maggior parte di esse appartiene al comparto della produzione del software e della consulenza informatica (divisione ATECO 62), sebbene vi sia una quota non marginale di rispondenti classificati in altri comparti. Le imprese concentrano le loro attività in Italia: oltre tre quarti dichiarano che il fatturato è generato per oltre il 90 per cento a livello nazionale. Le imprese che fanno capo a un'entità estera rappresentano circa il 20 per cento dei rispondenti. La struttura del mercato è dinamica, con diverse unità giovani o che negli ultimi anni hanno cambiato assetto societario.

L'offerta dei servizi di cybersicurezza e, in particolare, di testing. – La quasi totalità dei rispondenti dichiara di offrire servizi di cybersicurezza. Sulla base del numero degli addetti alle specifiche linee di business, si può desumere che tali servizi sono erogati sia da società specializzate che da società IT generaliste. Per circa un terzo di esse la *cybersecurity* è l'attività di gran lunga prevalente (oltre tre quarti del fatturato). Nell'ambito dei servizi di cybersicurezza, l'incidenza di quelli di testing in termini di fatturato si riduce al crescere della dimensione delle imprese. Il 44 per cento di quelle che offrono servizi di testing dichiara di avere oltre l'80 per cento del personale certificato in materia. Quattro rispondenti su cinque utilizzano l'intelligenza artificiale nell'offerta dei servizi di cybersicurezza, soprattutto nella *threat intelligence*. Quasi la metà delle società offre servizi a cinque o più tipologie di istituzioni finanziarie, delle quali le banche sono la più frequente.

L'offerta dei servizi di TLPT. – Circa il 70 per cento dei rispondenti offre o intende offrire servizi di tipo TLPT, con una percentuale più marcata per le imprese di maggiori dimensioni. In termini di numero di servizi erogati (di *threat intelligence* e/o *red teaming*), il settore è concentrato (indice di Gini pari a 0,7). Sulla base dei dati rilevati, nel 2023 l'offerta di questi servizi è cresciuta considerevolmente e due rispondenti su tre considerano il mercato in espansione. Tra i fattori che favorirebbero maggiormente lo sviluppo del mercato sono riportati la regolamentazione, l'adozione di framework pubblici e/o pubblico-privati, l'utilizzo di schemi di accreditamento e/o di certificazione delle imprese. Tra i principali ostacoli, invece, per l'80 per cento circa delle imprese figurano la limitata disponibilità di personale qualificato e il costo del servizio. Nell'erogazione dei servizi di TLPT emerge una forte variabilità nelle risorse impiegate per singolo servizio, in termini di giorni-uomo. Ciò evidenzia come non ci sia ancora un'offerta pienamente standardizzata: il TIBER-EU è il principale framework di riferimento, ma non è trascurabile l'utilizzo di metodologie proprietarie, segnalate da quasi un terzo delle società attive in quest'ambito.

[5] L'ATECO è la classificazione delle attività economiche adottata dall'Istat per finalità statistiche e rappresenta la versione italiana della nomenclatura europea NACE. Per l'indagine si è fatto riferimento alla classificazione ATECO 2007 aggiornamento 2022.

3. CONTESTO

Il contesto internazionale. – La *cyber resilience*[6] è una priorità per molti organismi internazionali e autorità finanziarie. Il World Economic Forum ha evidenziato nel rapporto sui rischi globali, che i problemi relativi alla sicurezza informatica sono uno dei principali rischi percepiti, nel breve e nel lungo termine (World Economic Forum, 2024). Il sistema finanziario è particolarmente esposto a malfunzionamenti di tipo tecnologico (ad esempio, il recente caso Crowdstrike) e rappresenta un obiettivo privilegiato di attacchi cibernetici. Anche il Meccanismo di vigilanza unico ha inserito la resilienza cibernetica tra le sue priorità di vigilanza[7].

Per quanto riguarda le infrastrutture dei mercati finanziari (*Financial Market Infrastructures*, FMIs), nel 2016 il Committee on Payments and Market Infrastructures e l'International Organization of Securities Commissions (congiuntamente CPMI-IOSCO) hanno definito la *Guidance on cyber resilience for financial market infrastructures* (CPMI-IOSCO, 2016), al fine di integrare i *Principles for Financial Market Infrastructures* (PFMI) (CPMI-IOSCO, 2012) in tema di resilienza cibernetica. La Guidance ha influenzato ulteriori lavori a livello nazionale e internazionale; inoltre, essa include specifiche indicazioni per i test di tipo *red team* nell'ambito delle linee guida sul testing in generale, che rappresentano una delle componenti fondanti del documento (*overarching component*). Sempre nel 2016 il G7 ha pubblicato i *Fundamental Elements of Cybersecurity for the Financial Sector*[8], richiamando l'importanza dei test nell'ambito di uno degli elementi principali della sicurezza: il monitoraggio.

Nel 2018 il G7 ha pubblicato i *Fundamental Elements for Threat-Led Penetration Testing*[9], che forniscono alle istituzioni finanziarie una guida per la valutazione della propria resilienza contro incidenti cyber malevoli attraverso delle simulazioni e alle autorità uno strumento per promuovere e armonizzare l'uso dei TLPT nelle varie giurisdizioni, tenendo in considerazione le peculiarità nazionali. Nello stesso anno sono stati pubblicati dal G7 anche i *Fundamental Elements for Third Party Cyber Risk Management in the Financial Sector* che, per far fronte allo sviluppo del settore e all'evoluzione delle minacce informatiche, sono stati rivisti nel 2022[10] con l'indicazione di includere esplicitamente nelle clausole contrattuali tra entità finanziarie e terze parti dei requisiti sulla frequenza e sui tipi di test di resilienza cibernetica (ad es. *penetration tests*, *threat-led penetration testing*).

Il contesto europeo. – Nel 2017 la BCE ha pubblicato la Strategia di resilienza cibernetica dell'Eurosistema per le FMI[11] con l'obiettivo di migliorare la resilienza cibernetica del settore finanziario nell'area dell'euro e di promuovere la collaborazione tra le stesse FMI, i loro fornitori di servizi critici e le autorità. La strategia, recentemente aggiornata[12], comprende diversi strumenti per verificare lo stato di preparazione delle entità finanziarie, tra cui il TIBER-EU, modello di riferimento per la conduzione di test avanzati di cybersicurezza armonizzati a livello europeo e adottato nel 2018 (Figura 3.1).

[6] È la capacità di un'organizzazione di continuare a svolgere i propri compiti anticipando e adattandosi alle minacce cyber e ad altri cambiamenti rilevanti nell'ambiente, e di resistere, contenere e riprendersi rapidamente dagli incidenti informatici (trad. da FSB, *Cyber lexicon*, 2023). Nel presente lavoro, cyber resilience, resilienza cibernetica e resilienza operativa digitale rappresentano lo stesso concetto.

[7] SSM Supervisory priorities and risk assessment for 2023-2025, *Priority 2: Addressing digitalisation challenges and strengthening management bodies' steering capabilities*.

[8] Cfr. G7 (2016).

[9] Cfr. G7 (2018).

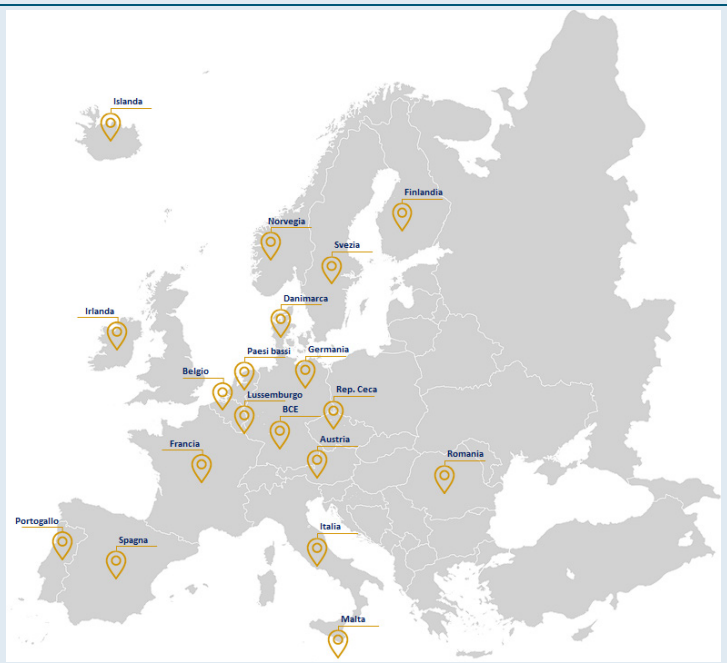
[10] Cfr. G7 (2022).

[11] Cfr. BCE (2017).

[12] Cfr. BCE (2024).

Figura 3.1

Paesi che hanno adottato il *framework* TIBER-EU



Fonte: elaborazioni su dati di BCE e del TIBER Knowledge Center.

Sul piano regolamentare, l'Unione europea ha recentemente adottato una serie di misure specifiche con il *Digital Operational Resilience Act* (DORA)[13], che stabilisce requisiti armonizzati per la gestione del rischio informatico per le varie tipologie di operatori del settore finanziario e introduce un regime di sorveglianza sui fornitori critici di servizi IT (cc.dd. terze parti critiche, cTPP). In merito al testing, viene richiesto alle entità finanziarie, identificate dalle autorità nazionali competenti, di eseguire almeno ogni tre anni test avanzati di tipo TLPT. Il processo e la metodologia che gli operatori devono utilizzare in questi test sono stati sviluppati dalle autorità di supervisione europee in conformità con il framework TIBER-EU. Con l'applicazione di DORA il TLPT è diventato a tutti gli effetti uno strumento di vigilanza, modificando l'attuale panorama rappresentato dal TIBER-XX[14], di solito basato su un approccio volontario per la maggior parte delle giurisdizioni che hanno contestualizzato il framework.

Anche la legislazione europea in tema di cybersicurezza, rivolta ad un ambito più ampio del solo settore finanziario, è stata recentemente aggiornata con la direttiva NIS2[15]. La Direttiva sottolinea l'importanza dei fornitori di servizi di sicurezza nel supportare le attività dei soggetti a cui forniscono i loro servizi, in ambiti quali la risposta agli incidenti, i *penetration test* e gli audit di sicurezza. Inoltre, i fornitori stessi possono essere vittime di attacchi cyber e, per tale motivo, dovrebbe essere posta particolare attenzione nella loro selezione.

Il contesto italiano. – In Italia il quadro regolamentare si è consolidato a partire dal recepimento della prima versione della direttiva NIS[16]; è stato definito il Perimetro di Sicurezza Nazionale Cibernetica (Perimetro) e istituita l'Agenzia per la Cybersicurezza Nazionale (ACN)[17]. Ad esempio,

[13] Regolamento (UE) 2022/2554 del Parlamento europeo e del Consiglio del 14 dicembre 2022 relativo alla resilienza operativa digitale per il settore finanziario e che modifica i regolamenti (CE) n. 1060/2009, (UE) n. 648/2012, (UE) n. 600/2014, (UE) n. 909/2014 e (UE) 2016/1011.

[14] Per TIBER-XX si intende una delle implementazioni nazionali del TIBER-EU. Ad esempio, il TIBER-IT, il TIBER-DE, il TIBER-NL.

[15] Direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio del 14 dicembre 2022 relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148 (direttiva NIS 2), recepita con il d.lgs. 138/2024.

[16] Direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio del 6 luglio 2016 recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione, recepita con il d.lgs. 65/2018.

[17] Si fa riferimento, rispettivamente, al d.l. 105/2019, convertito dalla l. 133/2019, e al d.lgs. 82/2021.

nell'elenco delle misure minime di sicurezza per gli operatori inclusi nel Perimetro si richiede che, almeno per le funzioni critiche, vengano eseguiti regolarmente dei *penetration test*. Questi atti sono intersettoriali e nell'ambito di applicazione includono una parte del settore finanziario.

Nell'agosto 2022 la Banca d'Italia, congiuntamente a Consob e Ivass, ha adottato il TIBER-IT[18], come contestualizzazione del TIBER-EU in una prospettiva di stabilità finanziaria (nell'ambito delle competenze affidate dall'ordinamento alle tre Autorità in materia di stabilità, efficienza e competitività del sistema finanziario, nonché di quelle di sorveglianza sul regolare funzionamento, affidabilità ed efficienza del sistema dei pagamenti). Il TIBER-IT è prioritariamente indirizzato alle entità finanziarie critiche per il sistema finanziario italiano tra le categorie seguenti:

- infrastrutture del mercato finanziario;
- sistemi di pagamento e infrastrutture di supporto tecnologico o di rete;
- sedi di negoziazione;
- banche;
- istituti di pagamento e di moneta elettronica;
- intermediari finanziari ex art. 106 del Testo unico bancario (TUB);
- imprese di assicurazione;
- intermediari assicurativi.

Fino a febbraio 2025, la Banca d'Italia ha supervisionato lo svolgimento di test volontari su 12 soggetti di diverse tipologie, tra cui banche, assicurazioni e altri operatori attivi nel sistema dei pagamenti (Scotti, 2025).

Ricerche di mercato nell'ambito della cybersecurity

Negli ultimi anni sono state pubblicate analisi e ricerche di mercato sulla cybersicurezza, condotte principalmente da enti privati e orientate ad analizzare la domanda di prodotti e servizi (il target sono le imprese in quanto clienti, non fornitori), gli investimenti effettuati dalle aziende o il livello di sicurezza percepito dalle aziende stesse.

L'indagine conoscitiva presentata in questo lavoro analizza il lato dell'offerta. Lavori analoghi sono stati svolti in una prospettiva settoriale, concentrando l'attenzione sui servizi offerti a una particolare industria o settore (ad esempio ENISA, 2022). Inoltre, come evidenziato dall'Agenzia dell'Unione europea per la cibersicurezza (ENISA), sebbene in passato la cybersicurezza sia stata presa in considerazione nelle analisi di mercato, la personalizzazione e l'ambito di questi approfondimenti sono ancora a un livello di maturità relativamente basso (ENISA, 2023).

Il contesto risente anche della mancanza di una specifica identificazione dei servizi di cybersicurezza nelle classificazioni delle attività economiche, sia a livello nazionale da parte dell'ISTAT sia nella classificazione NACE[19] di Eurostat.

In relazione alle analisi sugli investimenti effettuati dalle aziende, secondo l'ENISA *NIS Investments 2024 report*[20] le imprese nel 2023 destinavano alla sicurezza informatica il 9 per cento degli investimenti IT (con un aumento di 1,9 punti percentuali rispetto all'anno precedente) e l'11,1 per cento delle risorse IT a tempo pieno (FTE) (in calo di 0,8 punti percentuali rispetto al 2022). La media della spesa IT delle imprese si attestava a 98,5 milioni di euro (mediana 15 milioni); in posizione preminente era il settore bancario, con una spesa media di 222 milioni. L'investimento

[18] Cfr. Banca d'Italia, Consob e Ivass (2022).
[19] *Nomenclature statistique des activités économiques dans la Communauté européenne*.
[20] Il rapporto mira a fornire alle autorità di regolamentazione elementi concreti per valutare l'efficacia dell'attuale quadro normativo della UE in materia di cybersicurezza, in particolare attraverso dati sull'impatto della NIS sugli investimenti in cybersicurezza e sul livello complessivo di maturità dei soggetti cui la NIS è indirizzata.

medio in cybersicurezza delle imprese era di 6,75 milioni, sempre guidato dal settore bancario, con una media di 13,9 milioni. Il settore delle FMI, pur di dimensioni molto ridotte in termini di spesa complessiva, è il primo nel rapporto tra FTE destinati alla cybersicurezza e FTE totali del comparto IT (22,8 per cento in media). Più in generale, emerge una forte variabilità della spesa sia a livello intersettoriale che intra-settoriale. Infine, dal rapporto emerge che, in vista dell'applicazione di DORA, l'84 per cento delle imprese del settore bancario e del settore delle FMI dovranno assumere nuovo personale specializzato in cybersicurezza. Il divario di competenze è più elevato nell'area della cybersicurezza che comprende il testing ("*cybersecurity operations*").

Per l'Italia, una rilevazione degli investimenti IT del settore bancario è svolta dalla Convenzione Interbancaria per l'Automazione (CIPA) in collaborazione con l'Associazione Bancaria Italiana. Secondo la rilevazione sul 2023 (CIPA, 2024), il totale della spesa media IT dei gruppi bancari rispondenti è pari a 290,6 milioni, di cui 16,4 in media dedicati alla cybersicurezza, in aumento di circa il 9 per cento rispetto al 2022.

Secondo l'Osservatorio Cybersecurity e Data Protection del Politecnico di Milano (2024), il mercato della cybersicurezza in Italia negli ultimi anni è cresciuto costantemente (nel 2023 del 16 per cento rispetto all'anno precedente, attestandosi su un valore stimato di 2.146 milioni). Tra i principali fattori di crescita figurano le azioni di adeguamento alle nuove normative, tra cui DORA.

La stessa tendenza è confermata dai dati raccolti da Anitec-Assinform (2024). Gli investimenti in cybersicurezza delle imprese italiane sono stimati intorno a 1.790 milioni, in aumento del 12,2 per cento rispetto al 2022. La crescita maggiore ha interessato i settori della sanità e della pubblica amministrazione, mentre le banche investono in valore assoluto più degli altri comparti, in linea con le evidenze dell'ENISA. Tra i servizi offerti le attività di consulenza, che includono quelli come il testing, mostrano la spesa più contenuta (96,6 milioni, in aumento dell'11,8 per cento rispetto al 2022). Il report prevede per il 2024 una crescita notevole per tutto il comparto della cybersicurezza, guidata dalle normative che impongono l'adozione di misure specifiche in un numero sempre più esteso di settori.

Negli investimenti in ambito cybersicurezza è più indietro il comparto nazionale delle piccole e medie imprese (PMI), che presenta ampi margini di sviluppo. Dal Rapporto Cyber Index PMI 2023[21] emerge una correlazione tra la dimensione aziendale e il livello di maturità delle imprese. L'83 per cento delle PMI intervistate ricorre a strumenti digitali per supportare i processi aziendali, ma in quasi la metà dei casi non vi è un chiaro approccio strategico che coinvolga la proprietà e non sono stanziati fondi specifici per proteggere i sistemi informatici.

Nel 2021, in seguito all'adozione del Cybersecurity Act[22], l'ENISA ha avviato una serie di attività nel campo della ricerca di mercato sulla cybersicurezza con l'obiettivo di indagare anche il lato dell'offerta. Ad aprile 2022 è stato pubblicato il *Cybersecurity Market Analysis Framework* (ECSMAF), recentemente aggiornato (ENISA, 2023); esso rappresenta uno standard a livello europeo utilizzabile per definire, personalizzare e svolgere analisi di mercato.

L'indagine oggetto di questo lavoro si è avvalsa della metodologia dell'ENISA e ha preso in considerazione le relative indicazioni nelle varie fasi di esecuzione.

[21] Sviluppato nell'ambito delle attività previste dall'accordo siglato tra Confindustria, l'ACN e Assicurazioni Generali.

[22] Regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio del 17 aprile 2019 relativo all'ENISA, l'Agenzia dell'Unione europea per la cibersicurezza, e alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il regolamento (UE) n. 526/2013 («regolamento sulla cibersicurezza»).

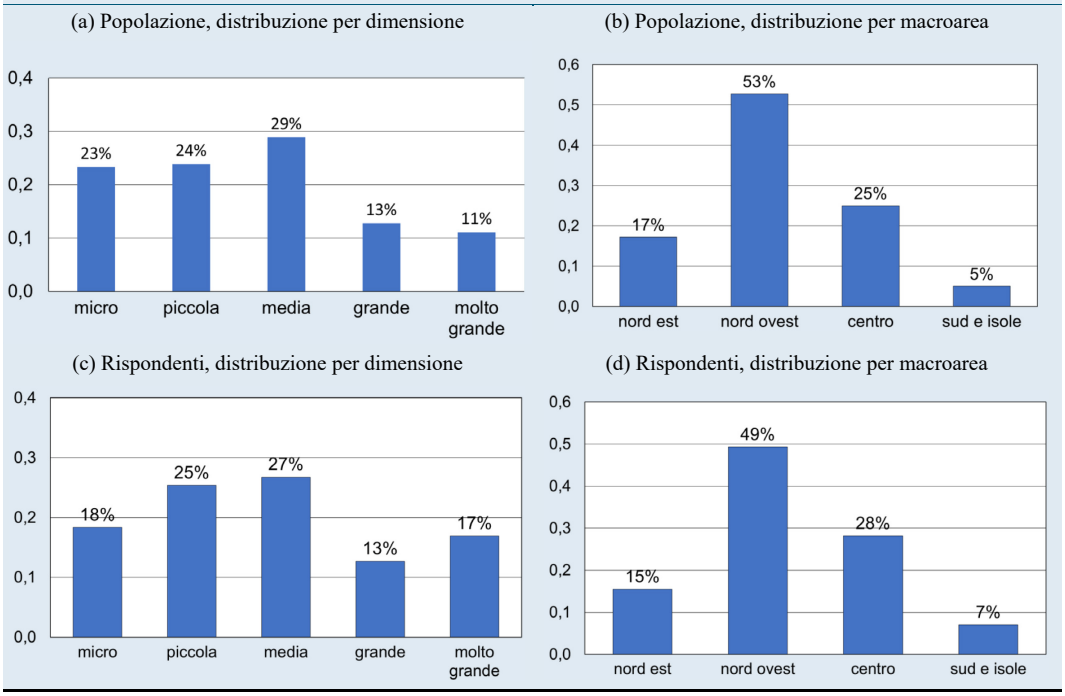
4. CARATTERISTICHE DELLE IMPRESE RISPONDENTI

Le imprese individuate. – È stato considerato un universo di riferimento di 180 imprese, costruito selezionando le imprese IT che forniscono servizi di testing di cybersicurezza o affini e con sede legale in Italia. Il processo di selezione si è reso necessario anche perché manca una tassonomia chiara e ufficiale delle attività del settore di interesse[23]. La ricognizione ha fornito un'indicazione della dimensione del settore, sebbene la lista di imprese individuate non vada considerata esaustiva, data la dinamicità di questo segmento di mercato[24]. I dettagli metodologici e i criteri adottati per la costruzione dell'universo di riferimento sono illustrati nella nota metodologica in Appendice A.

Per quanto riguarda la dimensione, le imprese sono state classificate secondo la raccomandazione 2003/361/CE[25], con l'aggiunta della categoria "molto grande" per le società con un fatturato maggiore di 100 milioni di euro[26]. La distribuzione delle 180 società su base dimensionale si discosta da quella delle imprese appartenenti alla sezione ATECO più vicina[27], visto che si distribuiscono in maniera omogenea tra le varie categorie dimensionali (Figura 4.1a). Dalla distribuzione della popolazione per macroarea geografica emerge come le società siano prevalentemente (70 per cento) concentrate nel Nord Italia, con un'alta concentrazione nel Nord Ovest (oltre la metà della popolazione, Figura 4.1b).

Figura 4.1

Confronto tra le distribuzioni della popolazione e dei rispondenti
Popolazione = 180 imprese; Rispondenti = 71 imprese;
(valori percentuali)



Fonte: elaborazioni su dati ORBIS.

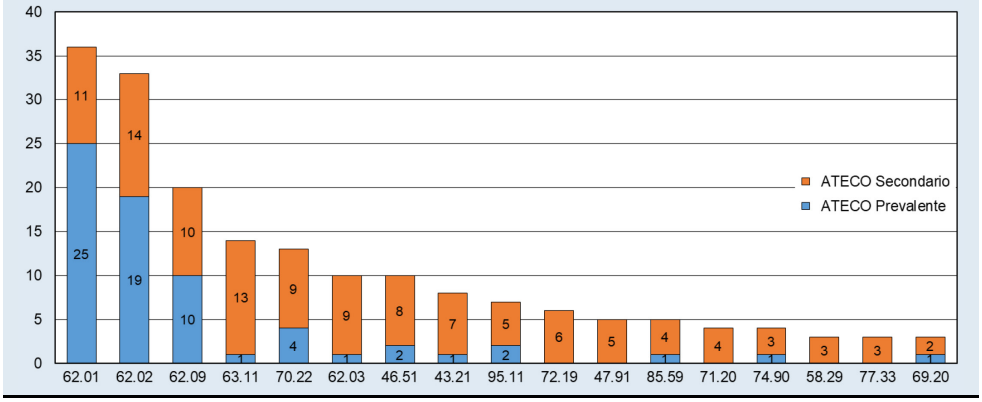
[23] Ad esempio, non è presente un codice ATECO che identifica puntualmente i servizi di testing di cybersicurezza.
[24] Durante la fase di implementazione dell'indagine, durata circa sei mesi, hanno cambiato assetto societario cinque imprese.
[25] La raccomandazione europea distingue tra "micro", "piccola" e "media" impresa per numero di dipendenti, attivo e fatturato. Le restanti imprese formano la categoria "grande". Le informazioni anagrafiche ed economiche sono state raccolte da varie fonti (Registro delle imprese, INPS e Orbis), con riferimento ai dati di fine 2023.
[26] Queste società formano un cluster distinto dalla categoria "grande". Il loro fatturato medio supera ampiamente quello delle altre grandi imprese, con un rapporto di 10 a 1.
[27] Si tratta della sezione "J - Servizi di informazione e comunicazione" e della classe "62.01 - Produzione di software non connesso all'edizione".

Le imprese rispondenti. – Al questionario hanno risposto 71 società, per un tasso di risposta del 39,4 per cento[28]. In termini di dimensione e area geografica non emergono differenze significative tra le frequenze delle distribuzioni delle società rispondenti e quelle della popolazione di riferimento (Figura 4.1c e Figura 4.1d). Anche altre variabili analizzate (ad es. l'anzianità dell'impresa) non mostrano distribuzioni significativamente diverse.

Codici ATECO delle imprese rispondenti. – La mancanza di un codice ATECO specifico per i servizi di cybersicurezza ha influenzato la perimetrazione dell'universo di riferimento. Tra i rispondenti si nota un'alta rappresentanza di imprese appartenenti alla divisione 62 ("Produzione di software, consulenza informatica e attività connesse") della sezione J ("Servizi di informazione e comunicazione"), distribuite in tutte le quattro classi previste (Figura 4.2 e Tabella 4.1)[29]. Non rientrano nella divisione 62[30] il 22 per cento dei rispondenti; tra questi, il codice prevalente è il 70.22[31].

Figura 4.2

Distribuzione dei codici ATECO delle imprese rispondenti
(unità)



Fonte: elaborazioni su dati InfoCamere e Orbis.
Note: ogni società possiede un solo codice ATECO prevalente e può avere uno o più codici secondari. Il grafico riporta i codici ATECO prevalenti e secondari con una ricorrenza complessiva maggiore o uguale a tre.

[28] Le analisi presentate non fanno sempre riferimento a tutti i 71 rispondenti, considerando che non tutte le domande erano obbligatorie e che, in alcuni casi, sono stati rimossi degli *outliers*. Nello specifico: i) due rispondenti per la domanda 9 della sezione TLPT: "Indicare il numero di Generic Threat Intelligence report (GTI) redatti nel 2022 e 2023"; ii) un rispondente per le domande 7 e 8 della medesima sezione, rispettivamente: "Indicare il numero di test TLPT per i quali sono stati forniti servizi nel 2022 e 2023" e "Indicare la percentuale di test TLPT per i quali sono stati offerti servizi al settore finanziario nel 2022 e 2023".

[29] Le classi 62.01 – "Produzione di software non connesso all'edizione", 62.02 – "Consulenza nel settore delle tecnologie dell'informatica", 62.03 – "Gestione di strutture informatizzate" e 62.09 – "Altre attività dei servizi connessi alle tecnologie dell'informatica".

[30] Le società che svolgono attività differenti da quelle prevalenti o primarie possono avere uno o più codici ATECO secondari.

[31] Il codice 70.22 è relativo alle attività "Consulenza imprenditoriale e altra consulenza amministrativo-gestionale e pianificazione aziendale", che si trova nella sezione M "Attività professionali, scientifiche e tecniche".

Tabella 4.1

Codice ATECO	Descrizione	Ricorrenza ATECO prevalente e secondario
62.01	Produzione di software non connesso all'edizione	36
62.02	Consulenza nel settore delle tecnologie dell'informatica	33
62.09	Altre attività dei servizi connessi alle tecnologie dell'informatica	20
63.11	Elaborazione dei dati, hosting e attività connesse	14
70.22	Consulenza imprenditoriale e altra consulenza amministrativo-gestionale e pianificazione aziendale	13
62.03	Gestione di strutture e apparecchiature informatiche hardware - housing (esclusa la riparazione)	10
46.51	Commercio all'ingrosso di computer, apparecchiature informatiche periferiche e di software	10
43.21	Installazione di impianti elettrici ed elettronici (inclusa manutenzione e riparazione)	8
95.11	Riparazione e manutenzione di computer e periferiche	7
72.19	Altre attività di ricerca e sviluppo sperimentale nel campo delle scienze naturali e dell'ingegneria	6
47.91	Commercio al dettaglio per corrispondenza o attraverso internet	5
85.59	Servizi di istruzione	5
71.20	Collaudi ed analisi tecniche; controllo di qualità e certificazione	4
74.90	Altre attività professionali, scientifiche e tecniche	4
58.29	Edizione di altri software a pacchetto (esclusi giochi per computer)	3
77.33	Noleggio di macchine e attrezzature per ufficio (inclusi i computer)	3
69.20	Contabilità, controllo e revisione contabile, consulenza in materia fiscale e del lavoro	3

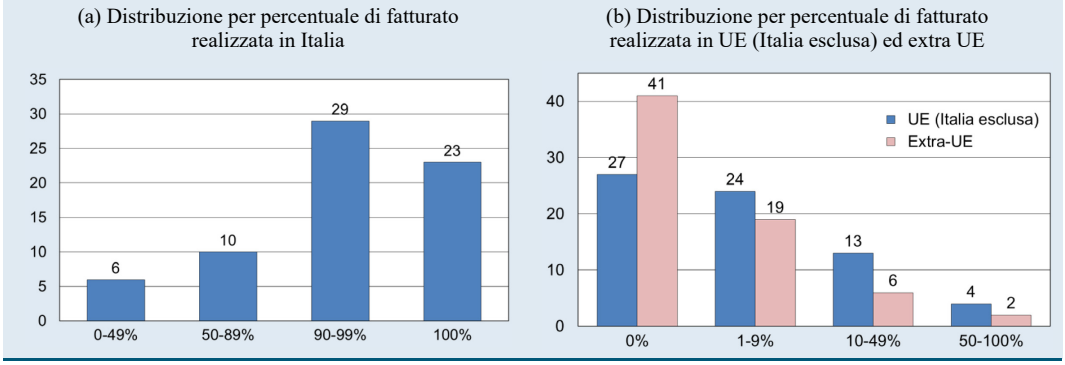
Struttura societaria. – Data la centralità del ruolo da essi svolto e la sensibilità dei dati trattati, i servizi per la cybersicurezza costituiscono un tassello fondamentale dell'autonomia tecnologica italiana, che, secondo la Strategia Nazionale di Cybersicurezza 2022-2026 (ACN, 2022b), è una delle sfide da affrontare nel settore del digitale, a livello nazionale ed europeo.

Il 56 per cento delle società rispondenti al questionario è parte di un gruppo societario e oltre la metà di questi gruppi ha sede in Italia. Le unità che fanno capo a un'entità estera rappresentano circa il 20 per cento dei rispondenti. Nel mercato italiano della cybersicurezza vi è dunque una prevalenza di operatori nazionali.

Fatturato. – Nell'analisi del fatturato vengono prese in considerazione tre aree geografiche: i) Italia; ii) Europa, Italia esclusa; iii) paesi extraeuropei (Figura 4.3). Il 33,8 per cento delle società realizza in Italia la totalità del fatturato, il 42,6 per cento ne realizza una quantità compresa tra il 90 e il 100 per cento. Pertanto, la gran parte dei ricavi delle società che operano nel mercato italiano dei servizi di cybersicurezza e di testing è prodotta sul mercato nazionale. Solo sei società hanno una quota di fatturato italiano inferiore al 50 per cento. Il 60 per cento delle società rispondenti non opera in paesi fuori dall'Unione; un altro 28 per cento non supera il 10 per cento di fatturato realizzato al di fuori dell'UE. Le imprese che generano ricavi nell'UE (esclusa l'Italia) o fuori dal continente per più della metà del fatturato sono una componente marginale (circa il 9 per cento dei rispondenti).

Figura 4.3

Distribuzione delle imprese per area geografica di fatturato (1)
(unità)

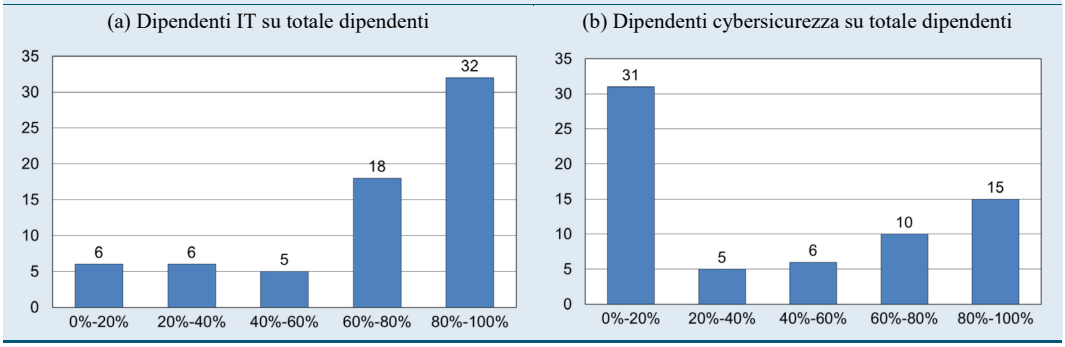


Fonte: elaborazioni su dati relativi a 68 rispondenti.
(1) Per le società appartenenti a gruppi, la distribuzione per area geografica si riferisce al fatturato della società, non della capogruppo.

Dipendenti specializzati in ambito IT. – Per il 74 per cento delle unità rispondenti la maggioranza dei dipendenti (più del 60 per cento) è impiegata in ambito IT, mentre circa la metà delle società (48 per cento) dichiara di utilizzarne la quasi totalità (tra 80 e 100 per cento); solo il 9 per cento dei rispondenti dichiara di avere meno del 20 per cento dei dipendenti impiegati nell'IT (Figura 4.4a). Prendendo in considerazione solo i servizi di cybersicurezza, invece, poco meno della metà dei rispondenti (46 per cento) dichiara di avere meno del 20 per cento dei dipendenti addetti a tali servizi, mentre questo utilizzo raggiunge la maggioranza per il 37 per cento delle imprese (Figura 4.4b). Prendendo il numero di dipendenti come *proxy* della specializzazione di una società in uno specifico settore o linea di business, si desume che nell'universo di riferimento i servizi di cybersicurezza sono erogati sia da società specializzate che da società IT generaliste.

Figura 4.4

Distribuzione delle imprese per fasce di rapporto tra dipendenti specializzati e dipendenti totali
(Unità)



Fonte: elaborazioni su dati relativi a 67 rispondenti.

5. OFFERTA DEI SERVIZI DI CYBERSICUREZZA E TESTING

Servizi di cybersicurezza

La quasi totalità delle società rispondenti (96 per cento) offre servizi di cybersicurezza[32]. La principale tipologia di servizio offerto è il testing (cfr. infra per dettagli), seguito da altri ad esso molto collegati (Figura 5.1). Ciò conferma l'adeguatezza del processo di costruzione dell'universo utilizzato per l'indagine. In particolare, le società di dimensioni grandi e molto grandi dichiarano di offrire tutti i servizi suddetti, dimostrando di avere un business diversificato in ambito di cybersicurezza.

Figura 5.1

I cinque servizi di cybersicurezza più offerti
(unità)

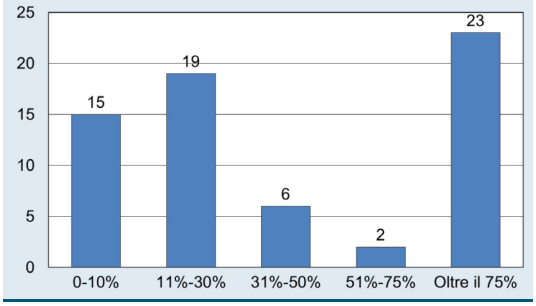
Fonte: elaborazioni su dati relativi a 68 rispondenti.

Utilizzo dell'intelligenza artificiale. – Quattro società su cinque offrono i servizi in discorso utilizzando tecnologie basate sull'intelligenza artificiale[33]. Questo dato va dal 60 per cento della macroarea del Sud e Isole all'85 per cento di quella del Nord Ovest. Tra i servizi di cybersicurezza quello per cui si ricorre maggiormente a soluzioni di intelligenza artificiale è quello di *threat intelligence*.

Fatturato dei servizi di cybersicurezza. – Essi rappresentano oltre il 75 per cento del fatturato totale per il 35 per cento delle società rispondenti (Figura 5.2). Le 23 società che si collocano in questa fascia, che sono dunque le più specializzate, offrono tutte l'intera gamma di servizi di cybersicurezza considerati nel questionario. Quasi due su tre sono micro e piccole imprese, le restanti sono medie e grandi imprese (non figurano imprese molto grandi). Pertanto, le imprese di grandi dimensioni, anche se offrono più tipi di servizi di cybersicurezza, realizzano su questo mercato una quota di fatturato più contenuta.

Figura 5.2

Distribuzione delle imprese per fasce di fatturato relativo a servizi di cybersicurezza
(unità)



Fonte: elaborazioni su dati relativi a 65 rispondenti.

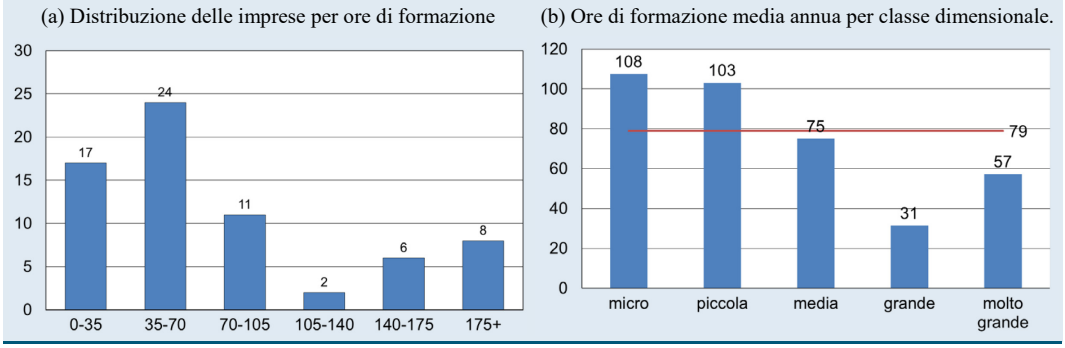
Formazione in cybersicurezza. – In materia di cybersicurezza le imprese rispondenti destinano in media 79 ore di formazione annua per dipendente (Figura 5.3a); il dato risente di alcune società particolarmente attive nell'ambito della formazione, con il 60 per cento dei rispondenti che destina meno di 70 ore. Investono relativamente di più in formazione le imprese più piccole (Figura 5.3b); tra le imprese grandi e molto grandi solo una dedica alla formazione più di 175 ore annue. Le ore medie a ciò dedicate aumentano al crescere della percentuale di dipendenti IT che si occupano di servizi di cybersicurezza; ad esempio, le imprese più specializzate (con oltre l'80 per cento di dipendenti IT addetti alla cybersicurezza) investono nella formazione IT una media di 126 ore annue per dipendente, mentre quelle meno specializzate (con una percentuale inferiore al 20 per cento) si attestano su una media di 57 ore.

[32] Sono stati presi in considerazione: Application Security; Cloud Security; Consumer Security; Data Security; ICS e Critical Infrastructure Security; Identity e Access Management; Integrated Risk Management; IoT e Embedded Security; Mobile Security; Network Security; Testing; Threat Intelligence; altro.

[33] Il dato è in linea con le tendenze di adozione di queste tecnologie nel settore bancario, dove si prevede una diffusione superiore al 90 per cento nell'impiego di IA generativa nell'ambito Documenti-contenuti e Governance, sicurezza, audit e compliance (CIPA, 2023).

Figura 5.3

Formazione in cybersicurezza nel 2023
(numero di imprese e ore medie di formazione annua per dipendente)

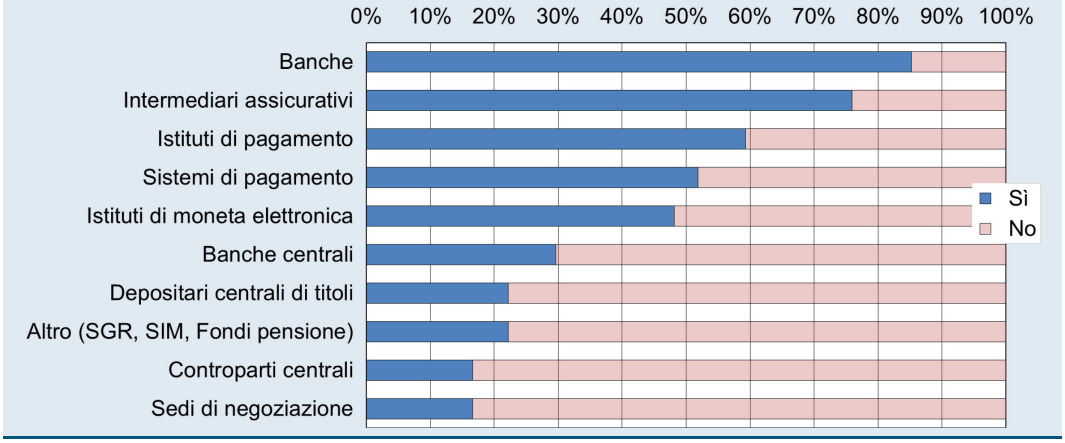


Fonte: elaborazioni su dati relativi a 68 rispondenti. Nella figura (b) la linea orizzontale rossa indica il valore medio.

Fornitura dei servizi di cybersicurezza. – Il 76 per cento dei rispondenti fornisce servizi di cybersicurezza al settore finanziario. Questa percentuale sale al 94 per cento per le imprese del Nord Ovest. Inoltre, tutte le imprese molto grandi offrono servizi al settore. Tra i clienti più ricorrenti si riscontrano, in ordine decrescente: banche, intermediari assicurativi e istituti di pagamento (Figura 5.4). Quasi la metà dei rispondenti (48 per cento) che offrono servizi di cybersicurezza al settore finanziario li offre a cinque o più tipologie di operatori.

Figura 5.4

Principali clienti dei servizi di cybersicurezza tra il settore finanziario
(valori percentuali)



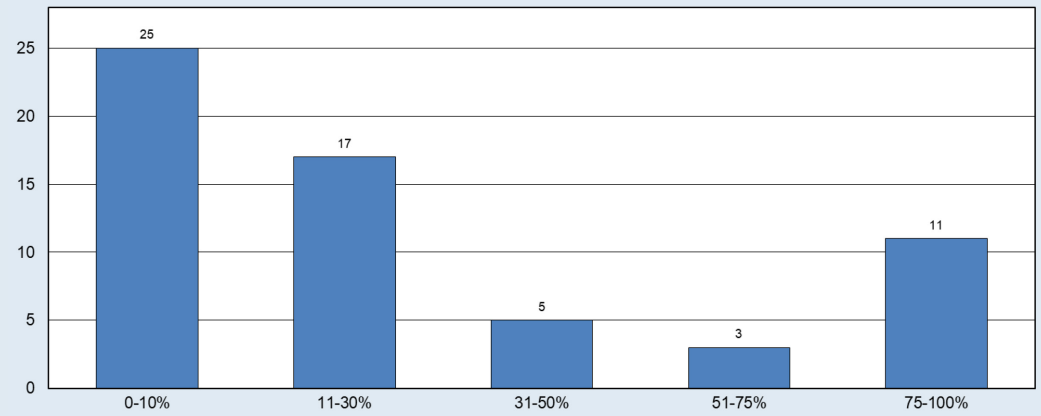
Fonte: elaborazioni su dati relativi a 54 rispondenti.

Servizi di testing

Il 93 per cento dei rispondenti offre servizi di testing di cybersicurezza. In generale, al crescere della dimensione delle imprese diminuisce la percentuale del fatturato del testing sul totale dei servizi di cybersicurezza. Tale quota è superiore al 30 per cento solo per una delle imprese della categoria "grande". Sette delle undici imprese che ricavano oltre il 75 per cento del fatturato dai servizi di testing (Figura 5.5) sono micro. Al crescere dell'anzianità diminuisce la quota percentuale di fatturato da testing, ma tra le 11 imprese più specializzate sono presenti sia unità costituite da meno di 5 anni sia unità che operano nel settore da oltre 20 anni.

Figura 5.5

Distribuzione delle imprese per percentuale del fatturato dei servizi di testing sul totale del fatturato dei servizi di cybersicurezza
(unità)



Fonte: elaborazioni su dati relativi a 61 rispondenti.

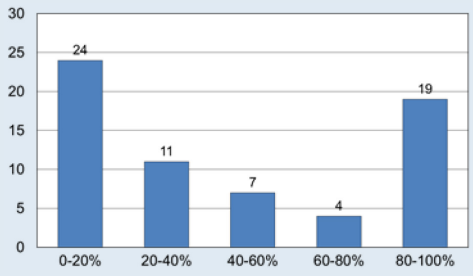
Inoltre, escludendo le imprese con una quota di fatturato da testing inferiore al 10 per cento (prima colonna della Figura 5.5), quasi il 90 delle unità restanti offre o ha in programma di offrire servizi di tipo TLPT al settore finanziario.

Una distribuzione simile si ritrova nell'incidenza dei servizi di testing in termini di percentuale dei dipendenti impiegati nei servizi di cybersicurezza (Figura 5.6); una quota di imprese consistente (29 per cento) è specializzata nelle attività di testing, con almeno quattro addetti in cybersicurezza su cinque.

Dalle risposte non emerge una dipendenza da un singolo cliente: per le imprese che offrono servizi di testing il cliente più rilevante pesa in media il 16 per cento del fatturato da testing, e nel 15 per cento dei casi il cliente principale contribuisce al fatturato per un valore maggiore del 30 per cento.

Figura 5.6

Distribuzione delle imprese per dipendenti che forniscono servizi di testing sul totale dei dipendenti di cybersicurezza
(unità)

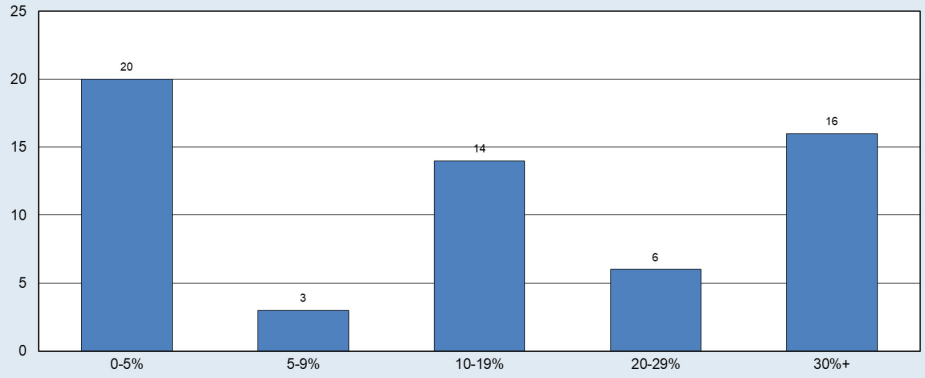


Fonte: elaborazioni su dati relativi a 65 rispondenti.

Il fatturato tra il 2022 e il 2023. – Per circa un terzo dei rispondenti il fatturato dei servizi di testing nel 2023 è cresciuto non più del 5 per cento, per il 40 per cento tra il 5 e il 29 per cento e per la parte restante di oltre il 30 (Figura 5.7). Complessivamente, dalle risposte emerge che il settore sta attraversando una fase di crescita in termini di fatturato, influenzata positivamente dall'erogazione di servizi di TLPT. Tra le imprese con maggiore crescita (più del 20 per cento) il 76 per cento dichiara di offrire questi servizi.

Figura 5.7

Distribuzione delle imprese per crescita del fatturato per i servizi di testing 2023 vs 2022
(unità)

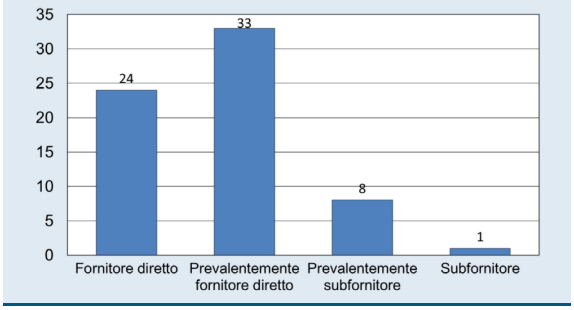


Fonte: elaborazioni su dati relativi a 59 rispondenti.

Modalità di fornitura dei servizi di testing. – I servizi in parola vengono offerti soprattutto in modo diretto (Figura 5.8). Meno di dieci rispondenti operano prevalentemente o completamente come subfornitori; tra questi figurano principalmente imprese di dimensioni minori, di cui solamente due offrono servizi nell'ambito TLPT.

Figura 5.8

Modalità di fornitura dei servizi di testing
(unità)

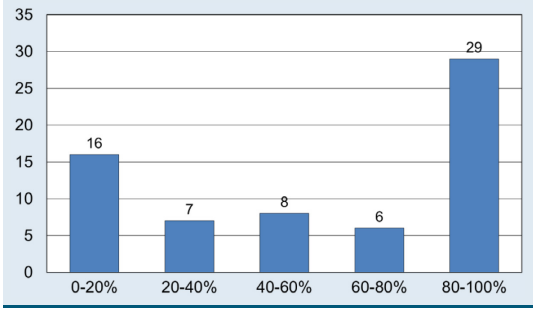


Fonte: elaborazioni su dati relativi a 66 rispondenti.

Personale certificato. – Il 44 per cento delle imprese che offrono servizi di testing ha oltre l'80 per cento del personale certificato in materia di cybersicurezza. Nel 24 per cento delle imprese il personale certificato è inferiore al 20 per cento (Figura 5.9). Le aziende con le più alte percentuali di personale certificato in media operano da più tempo (da 16-20 anni o da 20 anni e oltre).

Figura 5.9

Distribuzione delle imprese per fasce percentuali dei dipendenti certificati
(unità)



Fonte: elaborazioni su dati relativi a 66 rispondenti.

Tra le certificazioni che i rispondenti hanno segnalato[34] con più frequenza ricorrono quelle nell'ambito del testing e delle simulazioni di attacco, in particolare: Certified Ethical Hacker (60 per cento), Offensive Security Certified Professional (48 per cento) e eLearnSecurity Certified Professional Penetration Tester (39 per cento). Non mancano certificazioni indirizzate alla sicurezza informatica in generale, come, ad esempio, Certified Information Systems Security Professional (28 per cento). Tra quelle non presenti nella lista, le imprese hanno indicato Certified Information Security Manager, CompTIA Security+, Certified Red Team Professional, eLearnSecurity Web App Pen Tester eXtreme.

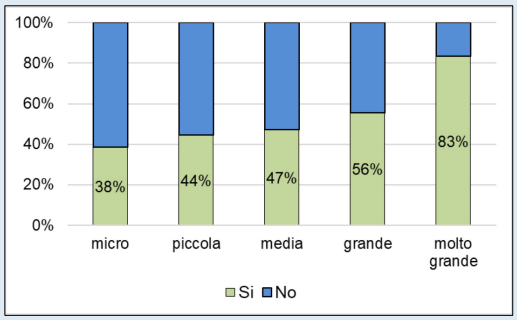
[34] Nel questionario era stata fornita la lista di certificazioni (ora rimossa) presente nelle TIBER-EU Services Procurement Guidelines, dando la possibilità di indicarne altre. La lista è utilizzata come elenco non esaustivo nel processo di acquisizione dei servizi per un test TIBER-EU.

6. OFFERTA DEI SERVIZI TLPT

Chi offre servizi di TLPT? – Il 52 per cento delle imprese intervistate offre servizi in ambito TLPT, che includono uno o entrambi i servizi di *threat intelligence* (*targeted* e/o *generic*) o di *red teaming*[35]. Tale percentuale aumenta al crescere della dimensione dell'impresa (Figura 6.1). Non è comunque trascurabile la presenza di imprese micro e piccole. Un ulteriore 20 per cento dei rispondenti dichiara che ha in programma di ampliare i servizi offerti includendo anche quelli relativi al TLPT. La fornitura di questo tipo di servizi non risulta condizionata dal settore di appartenenza delle imprese clienti (finanziario e non), il che configura questi servizi come trasversali. La disponibilità di un ampio bacino di clienti potenziali, provenienti da diversi ambiti produttivi, potrebbe favorire l'ulteriore espansione del settore, soprattutto alla luce delle nuove normative intersettoriali. Inoltre, occorre considerare che il framework TIBER-EU e le relative implementazioni nazionali, sebbene nati nell'alveo del settore finanziario, sono agnostici rispetto al comparto di applicazione e in alcune giurisdizioni sono stati già contestualizzati per altri settori (ad es. in quello delle *utilities*).

Figura 6.1

Fornitura dei servizi relativi al TLPT per dimensione dell'impresa
(Valori percentuali)

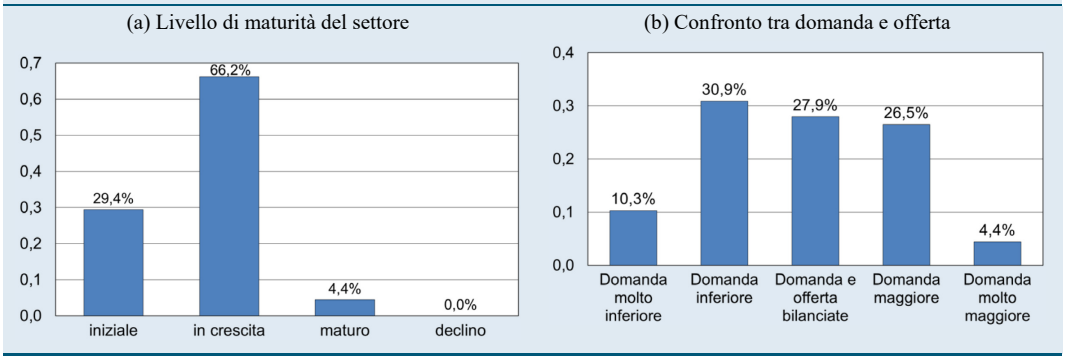


Fonte: elaborazioni su dati relativi a 71 rispondenti

Opinioni sul settore dei TLPT. – La quasi totalità dei rispondenti ritiene che il mercato si trovi in una fase iniziale o di crescita (Figura 6.2a). Per il 27,9 per cento domanda e offerta sono equilibrate (Figura 6.2b); per il resto prevalgono le percezioni di eccessi di offerta invece che di domanda (41,2 contro 30,9 per cento, rispettivamente). Le stesse valutazioni si riscontrano se si circoscrive l'analisi alle imprese che affermano di fornire i servizi di TLPT.

Figura 6.2

Fase di crescita del settore dei test di tipo TLPT
(valori percentuali)



Fonte: elaborazioni su dati relativi a 68 rispondenti.

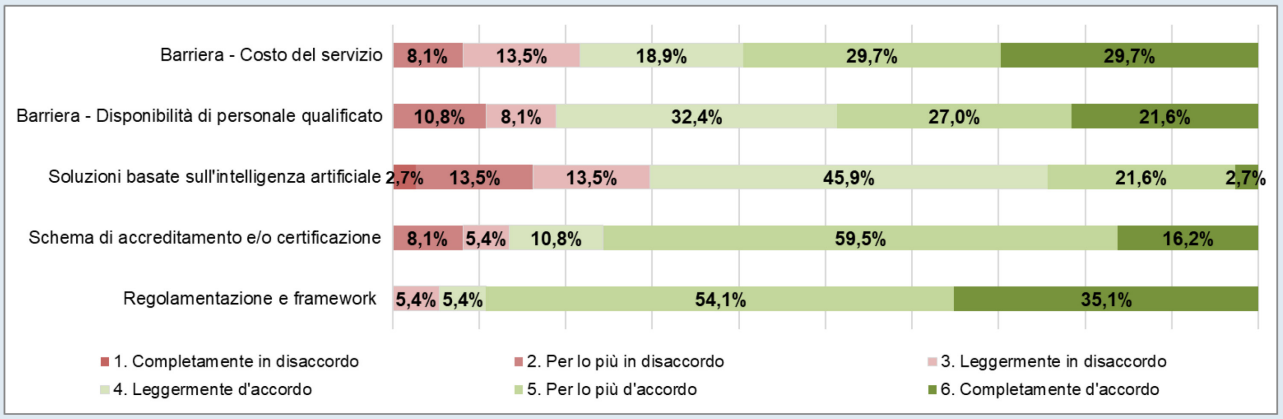
[35] Cfr. Appendice C - Glossario per le definizioni.

Per rilevare le opinioni dei rispondenti sulle principali tendenze del mercato del TLPT, sono state sottoposte alcune affermazioni per le quali è stato richiesto il livello di accordo o disaccordo secondo una scala di *Likert* a sei livelli[36]. I risultati (Figura 6.3) evidenziano come, secondo le imprese, i principali fattori che favorirebbero lo sviluppo del mercato sono la regolamentazione e l'adozione di framework pubblici e/o pubblico-privati (il 95 per cento circa delle imprese concorda con questa affermazione) e l'utilizzo di schemi di accreditamento e/o certificazione delle imprese che offrono i servizi in esame (l'86,5 per cento delle imprese ha risposto in area positiva). Questo risultato è simile alle evidenze raccolte dall'ENISA in un'analoga analisi del mercato dei servizi di cybersicurezza, però condotta dal lato della domanda (ENISA, 2024)[37].

Tra i principali ostacoli allo sviluppo del mercato l'80 per cento delle imprese rispondenti include il costo del servizio rispetto al budget dei clienti e la limitata disponibilità di personale qualificato; quest'ultimo è un tema noto e uno dei fattori abilitanti della strategia nazionale di cybersicurezza, per il quale sono previste varie misure nel relativo piano di implementazione (ACN, 2022a).

Figura 6.3

Principali barriere e driver per lo sviluppo del mercato
(Valori percentuali)



Fonte: elaborazioni su dati relativi a 37 rispondenti.

I servizi di TLPT erogati. – Le 37 imprese che offrono questi servizi di TLPT riportano di aver erogato nel 2023 318 servizi di TI o RT, con un forte incremento rispetto al 2022, quando ne avrebbero svolti 198. Stando ai dati del 2023 il settore sarebbe molto concentrato: un quarto delle società avrebbe erogato circa tre quarti dei servizi in ambito TLPT erogati dal totale dei rispondenti. Ciò è evidenziato dalla curva di Lorenz (Figura 6.4) e dall'indice di Gini, che per i servizi offerti nel 2022 e nel 2023 è pari a 0,7[38].

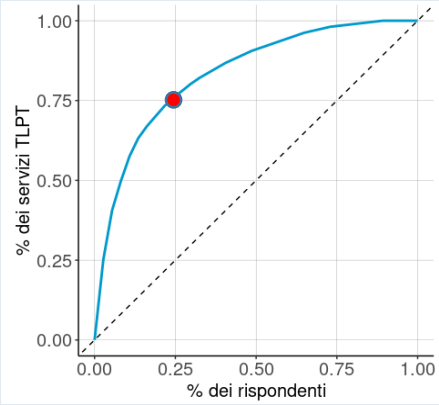
[36] 1. Completamente in disaccordo; 2. Per lo più in disaccordo; 3. Leggermente in disaccordo; 4. Leggermente d'accordo; 5. Per lo più d'accordo; 6. Completamente d'accordo.

[37] Infatti, tra le organizzazioni intervistate nell'analisi dell'ENISA, l'86 per cento ha dichiarato che una certificazione europea di cybersicurezza per prodotti con elementi digitali sarebbe vantaggiosa per il proprio settore. Inoltre, questo parere è particolarmente forte nel settore bancario, dove il 99 per cento degli intervistati da ENISA ne ha riconosciuto l'importanza.

[38] La curva di Lorenz è solitamente utilizzata per rappresentare la distribuzione delle disuguaglianze all'interno di una popolazione. L'indice di Gini fornisce il grado di disuguaglianza nella distribuzione di una variabile e si utilizza anche per misurare il grado di concentrazione di un fenomeno. L'indice varia tra 0 (uguaglianza perfetta) e 1 (massima disuguaglianza); si considera una concentrazione medio-alta se il suo valore è superiore a 0,5.

Figura 6.4

Concentrazione del mercato dei TLPT nel 2023 (1)
(valori percentuali)



Fonte: elaborazioni su dati relativi a 37 rispondenti.
(1) La linea celeste è la curva di Lorenz, che rappresenta la quota dei servizi TLPT offerti rispetto la quota dei rispondenti; il punto rosso indica il livello di concentrazione descritto nel testo.

Il settore finanziario è un cliente importante per i servizi TLPT. Sono stati erogati a entità finanziarie quasi un quarto dei test nel 2022 e oltre il 30 per cento nel 2023. Un fattore chiave nell'espansione del mercato può essere stata la spinta regolamentare. Inoltre, il principale quadro metodologico di riferimento per le imprese nell'erogazione dei servizi TLPT è il TIBER-EU: circa l'80 per cento delle imprese dichiara di offrire servizi TLPT per il TIBER-XX. Non è tuttavia neanche trascurabile l'utilizzo di metodologie proprietarie, segnalate dal 32 per cento dei rispondenti attivi in quest'ambito. Delle imprese che offrono servizi per i TLPT, solamente cinque dichiarano di essere certificate secondo schemi di accreditamento previsti per tali servizi, come il CBEST. A tal proposito si ricorda che al momento il TIBER-EU non prevede uno schema di accreditamento e certificazione. Il 51 per cento delle imprese aderisce a codici formali di condotta e/o etici specifici per le attività di TLPT.

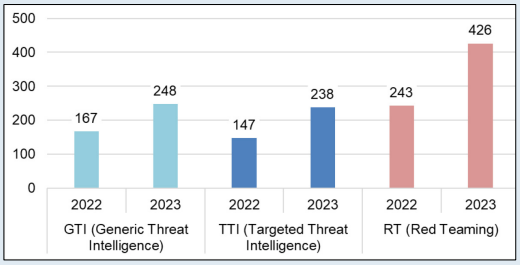
In generale, nel 2023 tutti i servizi relativi al TLPT hanno registrato una forte crescita, particolarmente pronunciata per quelli di *red teaming* (Figura 6.5a). In termini di risorse impiegate per singolo servizio, si registra una forte discrepanza tra la *threat intelligence* e il *red teaming*: in media 37 giorni-uomo per la prima, contro 69 per il secondo (Figura 6.5b). Dalle risposte si evidenzia anche che l'impiego di risorse è disomogeneo in relazione alla classe dimensionale dell'impresa, probabilmente a causa di una conduzione dei TLPT non ancora pienamente standardizzata tra le diverse realtà operative (con approcci e interpretazioni diverse delle procedure dei TLPT, se non delle stesse finalità). Va osservato che le imprese che dichiarano di offrire i servizi relativi ai TLPT secondo il framework TIBER-XX mostrano livelli di utilizzo delle risorse mediamente più alti: 43 giorni-uomo per la TI e 82 per l'RT.

In termini di esperienza del personale che guida l'esecuzione delle attività dei due servizi principali legati ai TLPT, un'elevata percentuale di imprese soddisferebbero il requisito relativo all'RT e al TI Manager presente sia nelle TIBER-EU Services Procurement Guidelines che negli RTS (*Regulatory Technical Standards*) di DORA sui TLPT (cinque anni). Gli anni di esperienza degli RT e TI Manager risultano superiori a tale soglia, rispettivamente, nell'82 e nel 57 per cento dei casi.

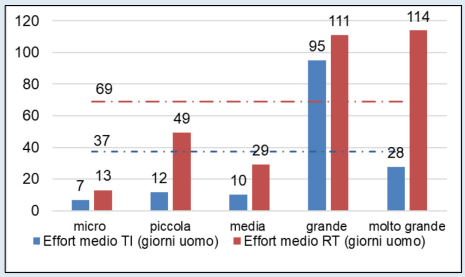
Figura 6.5

TLPT – Numeri e risorse impiegate nell'erogazione dei servizi

(a) Servizi erogati (*unità*)



(b) Risorse impiegate nei servizi di TI e RT (1) (*giorni-uomo*)



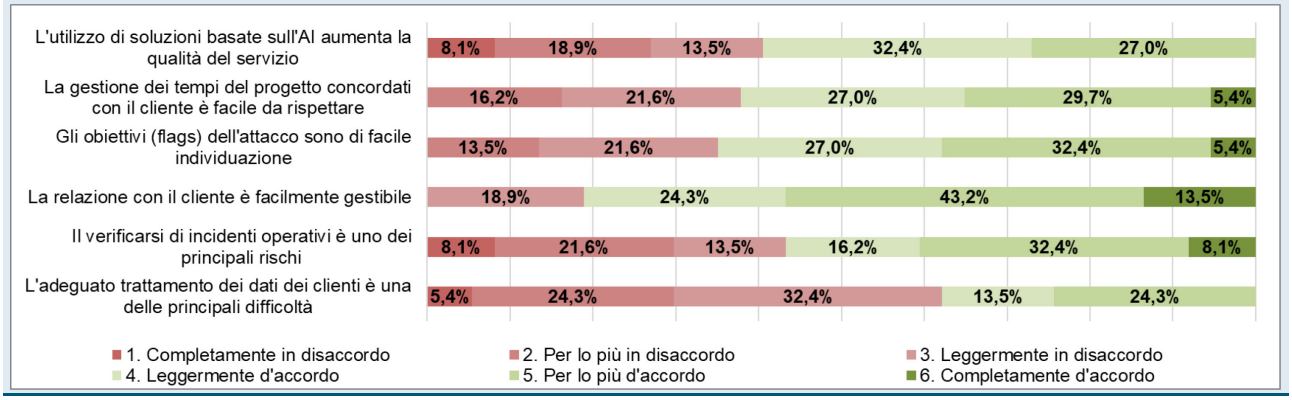
Fonte: elaborazioni su dati relativi a 37 rispondenti.
(1) Le linee orizzontali blu e rossa indicano il numero medio di giorni-uomo per i servizi di *threat intelligence* e di *red teaming*, rispettivamente.

Utilizzando la scala di Likert, è stata valutata l'opinione delle società su alcuni elementi di dettaglio della conduzione delle attività di TLPT (Figura 6.6). Il rapporto con il cliente risulta l'aspetto più semplice da gestire (86,5 per cento). Anche il trattamento dei dati dei clienti, spesso un tema delicato specialmente nell'ambito del *red teaming*, non risulta essere un elemento di particolare difficoltà nell'erogazione dei servizi. A tal proposito, da un'analisi della struttura societaria delle imprese rispondenti che eseguono attività di *red teaming* si evince che la loro proprietà è riconducibile nella maggioranza dei casi a un soggetto italiano. La capogruppo è domiciliata all'estero in circa un terzo dei casi[39]. Non risultano opinioni polarizzate in merito alla percezione del rischio del verificarsi di incidenti operativi durante le attività: solo una leggera maggioranza dei rispondenti (56,7 per cento) lo ritiene uno dei principali rischi. Ciò potrebbe essere dovuto alla richiesta di un'analisi del rischio pre-test e durante l'attività stessa, prevista dai vari framework metodologici. Inoltre, ad oggi, non risultano gravi incidenti derivanti dallo svolgimento di TLPT secondo il framework TIBER-EU, o una delle sue declinazioni nazionali.

Considerando la crescente attenzione e gli sviluppi recenti che hanno interessato l'intelligenza artificiale, dalle risposte non emergono opinioni polarizzate sui benefici che soluzioni di AI possono fornire ai servizi in discorso.

Figura 6.6

TLPT – Dettagli nell'erogazione del servizio
(Valori percentuali)



Fonte: elaborazioni su dati relativi a 37 rispondenti.

[39] L'analisi della struttura dei gruppi è basata su dati Orbis.

7. CONCLUSIONI

L'incidenza crescente dei rischi informatici nel settore finanziario ha indotto le autorità a rafforzare le azioni volte ad accrescere la resilienza operativa digitale dei singoli operatori e dell'intero sistema. Un traguardo significativo è la recente adozione del Regolamento DORA, che tra l'altro comporta per alcune tipologie di istituzioni finanziarie l'obbligo di svolgimento di test di tipo TLPT. Gli sviluppi delle tecnologie e della regolamentazione accrescono il ruolo delle imprese di servizi ICT e, in particolare, dei fornitori di servizi di cybersicurezza.

L'indagine oggetto di questo lavoro analizza l'offerta di questi servizi in Italia, differenziandosi quindi da altre analisi disponibili che si concentrano sul lato della domanda. Un primo risultato è che, sulla base delle classificazioni settoriali delle attività economiche attualmente in uso, le imprese che offrono servizi di cybersicurezza non sono associabili direttamente a comparti economici specifici. Pertanto, per perimetrare il mercato dal lato dell'offerta l'indagine ha combinato fonti informative diverse, quali liste di associazioni di settore, basi dati commerciali, dati a disposizione della Banca d'Italia (come il questionario Invind) e altre informazioni pubblicamente disponibili sulle singole società. Ne è risultato un universo di riferimento di circa 180 imprese. Il questionario è stato somministrato a tutte e 71 hanno risposto, con un tasso di risposta di circa il 40 per cento.

Dai risultati emerge la rapidità del cambiamento di questo mercato in Italia. A titolo esemplificativo, il 15 per cento delle imprese rispondenti è stato costituito o ha cambiato assetto societario negli ultimi cinque anni e, nei sei mesi di conduzione dell'indagine, cinque imprese sono state oggetto di fusioni o acquisizioni. Inoltre, tra quelle che hanno dichiarato di non offrire i servizi in parola la metà ha in programma di farlo nel prossimo periodo.

Nel mercato prevalgono gli operatori nazionali, in termini di assetto societario e per Paese di realizzazione del fatturato. Le società che fanno capo a un'impresa estera sono una su cinque.

Le strategie di offerta sono variegate. Alcune imprese offrono un'ampia gamma di servizi ICT, altre solo tipologie specifiche. Riguardo alle attività di testing, per quasi due imprese su tre esse generano meno del 30 per cento del fatturato, ma c'è un'ampia porzione di rispondenti (17 per cento) che risulta altamente specializzata, con una quota del fatturato superiore al 75 per cento.

Al momento i test di tipo TLPT rappresentano una quota minore delle attività di testing e sono molto concentrati: nel 2023 un quarto delle imprese attive hanno erogato i tre quarti dei servizi TLPT erogati dal totale dei rispondenti.

I dati inoltre evidenziano una forte variabilità nell'impiego di risorse e quindi nelle modalità di erogazione dei servizi di *red teaming* e *threat intelligence*. Queste differenze potrebbero essere attribuibili a diversi fattori: *i*) assenza di un modello di riferimento condiviso, almeno fino alla recente pubblicazione del TIBER-IT per il settore finanziario; *ii*) mancanza di uno schema di accreditamento o di certificazione a livello nazionale o europeo; *iii*) necessità di personalizzare il servizio per il cliente; *iv*) disomogeneità della domanda.

La notevole differenziazione delle esigenze della clientela e della disponibilità di risorse economiche, nonché le competenze tecniche richieste per eseguire queste attività si riflettono nell'impegno (in termini di giorni-uomo) per effettuare i TLPT. In alcuni casi, ciò potrebbe indicare che le attività sono svolte in modo più simile a un tradizionale *penetration test*, che richiede generalmente meno risorse, essendo molto più limitato sia nel perimetro da testare che nella durata; inoltre, un *penetration test* tradizionale non prevede l'utilizzo della *threat intelligence*.

Con la leva normativa, a livello europeo e nazionale, le autorità - finanziarie e non - stanno favorendo l'affermazione di modelli di riferimento per il mercato dei TLPT da cui potrebbe derivare una maggiore uniformità dei servizi erogati. Ad esempio, circa l'80 per cento delle imprese che svolgono TLPT dichiara di seguire il framework TIBER-EU. La gran parte delle società concorda che l'introduzione di schemi di accreditamento e di certificazione agevolerebbe la crescita del mercato e ne auspica l'introduzione. Il tema dello sviluppo di questi schemi per il TLPT è presente

in DORA ed è all'attenzione del TIBER Knowledge Center della BCE. Più in generale, sulla certificazione dei servizi di sicurezza gestiti (*managed security services*), che comprendono tra l'altro anche i *penetration test*, sono in corso valutazioni del regolatore europeo nell'ambito del Cyber Security Act. Essa favorirebbe una maggiore omogeneità sia nell'offerta sia nella domanda, con effetti anche sulla competitività del mercato.

RIFERIMENTI BIBLIOGRAFICI

ACN, Agenzia per la Cybersicurezza Nazionale (2022a), *Piano di implementazione - Strategia nazionale di cybersicurezza 2022-2026,* maggio 2022.

ACN, Agenzia per la Cybersicurezza Nazionale (2022b), *Strategia Nazionale di Cybersicurezza 2022-2026,* maggio 2022.

Anitec-Assinform (2024), *Il digitale in Italia 2024 - Mercati, dinamiche e policy*.

Banca d'Italia, Consob e Ivass (2022), *Guida nazionale TIBER-IT: Threat Intelligence Based Ethical Red-Teaming – Italia*, agosto 2022.

BCE, Banca Centrale Europea (2017), *Cyber resilience and financial market infrastructures*, marzo 2017.

BCE, Banca Centrale Europea (2018), *TIBER-EU FRAMEWORK*, maggio 2018.

BCE, Banca Centrale Europea (2024), *Eurosystem Cyber Resilience Strategy*, ottobre 2024.

CIPA, Convenzione Interbancaria Per l'Automazione (2024), *Rilevazione sull'IT nel settore bancario italiano - Profili economici e organizzativi - esercizio 2023*.

CPMI-IOSCO, Committee on Payments and Market Infrastructures - International Organization of Securities Commissions (2016), *Guidance on cyber resilience for financial market infrastructure*, giugno 2016.

CPSS-IOSCO, Committee on Payment and Settlement Systems - International Organization of Securities Commissions (2012), *Principles for financial market infrastructures*, aprile 2012.

ENISA, European Union Agency for Cybersecurity (2022), *EU Cybersecurity Market Analysis - IoT in Distribution Grids*, aprile 2022.

ENISA, European Union Agency for Cybersecurity (2023), *Cybersecurity market analysis framework V2.0*, marzo 2023.

ENISA, European Union Agency for Cybersecurity (2024), *NIS investments 2024*, novembre 2024.

FMI, Fondo Monetario Internazionale (2024), *Global financial stability report*, aprile 2024.

G7 (2016), *G7 Fundamental elements of cybersecurity for the financial sector*, ottobre 2016.

G7 (2018), *G7 Fundamental elements for threat-led penetration testing*, ottobre 2018.

G7 (2022), *G7 Fundamental elements for third party cyber risk management in the financial sector*, ottobre 2022.

Politecnico di Milano (2024), *Lo scenario della cybersicurezza in Italia nel 2023*.

Scotti C. (2025), *I test di tipo TLPT: dalle esperienze del TIBER-IT alle regole di DORA*, intervento al convegno della Banca d'Italia: "*THREAT-LED PENETRATION TESTING: dalle esperienze TIBER-IT alle regole sui TLPT di DORA",* febbraio 2025.

World Economic Forum (2024), *Global risks report*, gennaio 2024.

APPENDICE A – NOTA METODOLOGICA

Questa nota presenta le principali caratteristiche metodologiche dell'indagine conoscitiva. Si descrivono i criteri di individuazione dell'universo di riferimento e delle sue caratteristiche e le principali informazioni richieste tramite la somministrazione di un questionario (cfr. Appendice B).

La composizione dell'universo di riferimento

L'universo di riferimento dell'indagine si compone di società attive, con sede in Italia e operanti nel settore IT che offrono servizi di test di cybersicurezza o affini, fatta eccezione per: i) le società di persone (che si suppone siano meno propense a offrire servizi complessi come il TLPT); ii) società riconducibili a entità finanziarie.

Per il processo di costruzione dell'universo di riferimento si è utilizzato un approccio mirato data l'assenza di criteri di selezione specifici nelle classificazioni standard delle attività economiche. Infatti, considerata la classificazione ATECO, il mercato oggetto di analisi è presumibilmente compreso nella sezione J - "Servizi di informazione e comunicazione", che conta circa 40 mila imprese, ma non è associato direttamente a una specifica divisione, gruppo, classe, categoria o sottocategoria (codice ATECO). I codici ATECO riconducibili al settore ICT o alla consulenza informatica[40] sono stati utilizzati come filtro per effettuare delle interrogazioni sul Registro delle imprese. Si è giunti ad una lista di significative dimensioni (oltre 18 mila imprese), contenente molte società genericamente attive nel settore ICT ma non direttamente coinvolte nei servizi di cybersicurezza.

Di conseguenza, per delimitare l'universo dell'indagine, ovvero la lista delle imprese da contattare, si è proceduto con un'analisi combinando varie fonti:

- associazioni di settore: società presenti nelle liste pubbliche di associazioni di settore[41];
- basi dati commerciali: società identificate applicando come filtri, nei campi di descrizione delle attività, parole chiave relative ai servizi di cybersicurezza e al testing[42];
- questionario INVIND svolto nel 2023[43]: società che hanno risposto positivamente a una specifica domanda relativa all'offerta di servizi di cybersicurezza inserita nel questionario;
- informazioni già raccolte dalla Banca d'Italia sui fornitori ICT delle entità finanziarie[44]. Va al riguardo sottolineato che, dal punto di vista regolamentare, i servizi di interesse per l'indagine non sono soliti essere inquadrati come esternalizzazioni.

Tale processo ha portato all'individuazione di un sottoinsieme di 633 imprese. Su quest'ultimo si è svolta un'analisi dettagliata e manuale a livello di singola impresa, basata su tutte le informazioni disponibili, compresi i relativi siti *web* ufficiali, al fine di circoscrivere il più possibile l'insieme alle sole società che dichiarano di svolgere servizi di test di cybersicurezza o affini.

---

[40] In particolare si tratta della sezione J – "Servizi di informazione e comunicazione", classi 62.01, 62.02 e sottocategoria 62.09.09, rispettivamente "Produzione di software non connesso all'edizione", "Consulenza nel settore delle tecnologie dell'informatica" e "Altre attività dei servizi connessi alle tecnologie dell'informatica".

[41] Ad esempio: i) CLUSIT: Associazione Italiana per la Sicurezza Informatica; ii) ASSINTEL: Associazione nazionale delle imprese ICT; iii) AIPSA: Associazione Italiana Professionisti Security Aziendale.

[42] La ricerca è stata condotta sulle basi dati Bloomberg e Orbis filtrando per i codici ATECO della divisione 62 e/o per parole chiave, ad es.: Cyber, Cybersecurity, Penetration test, Threat intelligence, Red team, CBEST, TLPT e Tiber.

[43] Si tratta di un'indagine annuale condotta dalla Banca d'Italia sulle imprese industriali e dei servizi. Nel sondaggio INVIND è stata inserita la seguente domanda, indirizzata solamente alle società operanti in determinati codici ATECO: "La vostra azienda offre servizi di cybersecurity (ad esempio, threat intelligence, penetration test, red teaming, TLPT)?".

[44] Tale lista è costruita sulla base delle informazioni provenienti dai contratti di esternalizzazione conclusi tra le entità finanziarie e i fornitori.

Questa ulteriore scrematura ha portato a comporre un universo di riferimento per questa indagine di 185 società. Nel corso dell'indagine la popolazione si è ridotta a 180 imprese per alcuni cambiamenti negli assetti societari.

Confronto tra popolazione e rispondenti

Per verificare che la distribuzione delle imprese della popolazione e quelle dei rispondenti siano simili per quanto riguarda le principali variabili di studio, classificazione dimensionale e macroarea geografica, si è utilizzato il test *chi quadrato*[45]. Si riportano di seguito le tabelle delle frequenze osservate e di quelle attese per le due variabili considerate, con P=180 che rappresenta il numero delle imprese della popolazione e R=71 il numero dei rispondenti.

Le frequenze attese sono calcolate come: $e_i = (p_i/P) \times R$ dove p_i è la popolazione relativa alla categoria di riferimento.

Tabella A.1

Classe Dimensionale	p_i (popolazione)	o_i (rispondenti)	e_i (frequenze attese)
Micro	42	13	16,57
Piccola	43	18	16,96
Media	52	19	20,51
Grande	23	9	9,07
Molto grande	20	12	7,89

Tabella A.2

Macroarea Geografica	p_i (popolazione)	o_i (rispondenti)	e_i (frequenze attese)
Nord Ovest	95	35	37,47
Nord Est	31	11	12,23
Centro	45	20	17,75
Sud e Isole	9	5	3,55

La variabile di test X^2 si ricava sommando gli scarti quadratici tra le frequenze osservate (o_i) e quelle attese (e_i), pesato per le frequenze attese. L'ipotesi nulla di indipendenza, ovvero l'ipotesi che le due distribuzioni per dimensione e macroarea non dipendano dalle risposte ricevute e che quindi le frequenze dei valori osservati si adattano alle frequenze attese, è dimostrata se la variabile di test è minore del valore della distribuzione chi quadrato con k-1 gradi di libertà e un errore tollerato fissato a α=0,05. Nel caso della variabile classe dimensionale, k=5 e i gradi di libertà sono pari a 4. Per la variabile macroarea geografica, k=4 e i gradi di libertà sono pari a 3.

$$\chi^2 = \sum_{i=1}^{k} \frac{(o_i - e_i)^2}{e_i}$$

Il valore di riferimento della distribuzione del chi quadrato per 4 gradi di libertà è 9,49; per 3 gradi di libertà è 7,82. In entrambi i casi, i valori di X^2, 3,09 per la variabile classe dimensionale e 1,16 per la variabile macroarea geografica, risultano inferiori alle soglie; si può affermare che l'ipotesi nulla non è rifiutata e che quindi non vi sono differenze significative tra le distribuzioni di popolazione e rispondenti.

[45] In sintesi, l'obiettivo del test è quello di verificare che le frequenze dei valori osservati nei rispondenti non siano differenti statisticamente da quelle attese.

APPENDICE B – STRUTTURA DEL QUESTIONARIO

Sezione 1. Informazioni generali	
Numero della domanda	*Testo della domanda*
1	Indicare il nome dell'organizzazione.
2	Inserire la Partita Iva dell'organizzazione
3	Se l'organizzazione fa parte di un gruppo, inserire anche il nome della capogruppo.
	Se l'organizzazione fa parte di un gruppo, inserire anche la nazionalità della capogruppo.
4	Inserire il nome e cognome del responsabile per la compilazione del questionario.
	Inserire l'indirizzo email del responsabile per la compilazione del questionario.
	Inserire il numero di telefono del responsabile per la compilazione del questionario.
	Inserire il ruolo aziendale del responsabile per la compilazione del questionario.
5	Ai fini del questionario se non diversamente specificato si fa riferimento all'ultimo anno fiscale disponibile. Indicare la data di chiusura dell'ultimo anno fiscale disponibile.
6	Indicare una stima della distribuzione geografica del fatturato dei servizi IT forniti dall'organizzazione ai propri clienti nell'ultimo anno fiscale disponibile: • In Italia • Nell'Unione Europea (Italia Inclusa) • Nel resto del mondo
7	Qual è il numero totale dei dipendenti che forniscono servizi IT (inclusi i servizi di cybersicurezza) al 31-12-23?
Sezione 2. Servizi di cybersicurezza	
Numero della domanda	*Testo della domanda*
1	L'organizzazione fornisce servizi di cybersicurezza?

2	Selezionare le tipologie di servizi di cybersicurezza forniti: • Application Security • Cloud security • Consumer security • Data Security • ICS e critical infrastructure security • Identity & Access Management • Integrated Risk Management • IoT e embedded security • Mobile security • Network security • Testing (inclusi VA, PT, Red Teaming, etc) • Threat intelligence • Altro
3	Indicare la percentuale di fatturato relativa ai sevizi di cybersicurezza sul fatturato totale nell'ultimo anno fiscale disponibile.
4	Indicare il numero dei dipendenti che forniscono servizi di cybersicurezza al 31-12-23.
5	Indicare il numero medio di ore di formazione relative servizi di cybersicurezza erogate nel 2023 per singolo dipendente che fornisce servizi di cybersicurezza.
6	Indicare se si offrono servizi di cybersicurezza al settore finanziario. In tal caso indicare la tipologia delle entità finanziarie clienti: • Non vengono offerti servizi al settore finanziario • Banche • Istituti di moneta elettronica • Istituti di pagamento • Sistemi di pagamento • Infrastrutture di mercato • Sedi di negoziazione • Intermediari assicurativi • Banche centrali • Altro
7	Indicare se l'organizzazione utilizza soluzioni basate sull'intelligenza artificiale nell'erogazione dei servizi di cybersicurezza.
8	Selezionare le tipologie di servizi per i quali si utilizzano soluzioni basate sull'intelligenza artificiale: • Application Security • Cloud security • Consumer security • Data Security • ICS e critical infrastructure security • Identity & Access Management • Integrated Risk Management • IoT e embedded security • Mobile security • Network security • Testing (inclusi VA, PT, Red Teaming, etc) • Threat intelligence • Altro

Sezione 3. Servizi di testing	
Numero della domanda	*Testo della domanda*
1	L'organizzazione fornisce servizi di testing di cybersicurezza?
2	Indicare la percentuale di fatturato dei servizi di testing di cybersicurezza rispetto al fatturato riferito ai soli servizi di cybersicurezza nell'ultimo anno fiscale disponibile.
3	Indicare una stima della variazione del fatturato dei servizi di testing di cybersicurezza confrontando l'ultimo anno fiscale disponibile con il precedente.
4	Indicare una stima della percentuale del fatturato proveniente dal cliente più rilevante per i servizi di testing di cybersicurezza nell'ultimo anno fiscale disponibile.
5	Indicare il numero di dipendenti che forniscono servizi di testing di cybersicurezza al 31-12-23.
6	Tenendo conto del numero totale di dipendenti che forniscono servizi di testing di cybersicurezza, indicare la percentuale di personale certificato in materia di test di cybersicurezza al 31-12-23.
7	Selezionare le certificazioni possedute dai dipendenti di cui alla domanda precedente: • Certified Ethical Hacker • Certified Information Systems Security Professional • CREST Certified Infrastructure Tester • CREST Certified Simulated Attack Manager • CREST Certified Simulated Attack Specialist • CREST Certified Threat Intelligence Manager • CREST Registered Threat Intelligence Analyst • Cybersecurity Nexus • EC-Council Certified Security Analyst • eLearnSecurity Certified Professional Penetration Tester • GIAC Accessing and Auditing Wireless Networks • GIAC Advanced Penetration Tester • GIAC Cyber Threat Intelligence • GIAC Gold Cyber Threat Intelligence • GIAC Mobile Device Security Analyst • GIAC Penetration Tester • GIAC Web Application Penetration Testing • Licensed Penetration Tester • Offensive Security Certified Expert • Offensive Security Certified Professional • Offensive Security Exploitation Expert • Offensive Security Web Expert • Offensive Security Wireless Professional • Systems Security Certified Practitioner • Altro
8	Indicare la modalità prevalente con cui l'organizzazione fornisce servizi di testing di cybersicurezza.
Sezione 4. Servizi di TLPT	

Numero della domanda	*Testo della domanda*
1	L'organizzazione fornisce servizi di cybersicurezza di tipo Threat-Led Penetration Testing (TLPT)?
2	L'organizzazione programma di fornire servizi di TLPT al settore finanziario?
3	Indicare la tipologia di framework TLPT per i quali vengono offerti servizi: • CBEST (UK) • TIBER-EU / TIBER-XX • ICAST (HK) • AASE (ABS-SG) • REDFIN (IT) • CORIE (AUS) • FEERET (SA) • PTFSI (GFMA) • Proprietario • Altro
4	L'organizzazione è certificata secondo gli schemi di accreditamento previsti per i servizi di TLPT da alcuni framework di tipo pubblico e/o privato (ad esempio CBEST)? Indicare gli schemi di accreditamento per cui l'organizzazione è certificata.
5	Indicare una stima della percentuale di fatturato relativo ai servizi di TLPT nell'ultimo anno fiscale disponibile rispetto al fatturato totale dei servizi di cybersicurezza.
6	Indicare una stima della variazione del fatturato dei servizi di TLPT confrontando l'ultimo anno fiscale disponibile con il precedente.
7	Indicare il numero di test TLPT per i quali sono stati forniti servizi nel 2022. Indicare il numero di test TLPT per i quali sono stati forniti servizi nel 2023.
8	Indicare la percentuale di test TLPT per i quali sono stati offerti servizi al settore finanziario nel 2022. Indicare la percentuale di test TLPT per i quali sono stati offerti servizi al settore finanziario nel 2023.
Threat Intelligence	
9	Indicare il numero di Generic Threat Intelligence report (GTI) redatti nel 2022. Indicare il numero di Generic Threat Intelligence report (GTI) redatti nel 2023.
10	Indicare il numero di test TLPT per cui si è svolto il ruolo di fornitore di threat intelligence nel 2022 (ad esempio producendo il Targeted Threat Intelligence report - TTI). Indicare il numero di test TLPT per cui si è svolto il ruolo di fornitore di threat intelligence nel 2023 (ad esempio producendo il Targeted Threat Intelligence report - TTI).
11	Indicare l'effort medio complessivo di risorse umane per i servizi di targeted threat intelligence utilizzate per un singolo TLPT.
12	Indicare gli anni di esperienza media del TI team manager in attività di threat intelligence.
Red teaming	

13	Indicare il numero di test TLPT per cui si è svolto il ruolo di fornitore di red team nel 2022 (ad esempio producendo il Red Team Test Report - RTTR). Indicare il numero di test TLPT per cui si è svolto il ruolo di fornitore di red team nel 2023 (ad esempio producendo il Red Team Test Report - RTTR).
14	Indicare l'effort medio complessivo di risorse umane, per il servizio di red teaming per un singolo TLPT.
15	Indicare gli anni di esperienza media del RT team manager in attività di red teaming.
16	Indicare se l'organizzazione ha sottoscritto assicurazioni specifiche per lo svolgimento di servizi di TLPT.
17	Se l'organizzazione effettua attività di ricerca in ambito di sicurezza, indicare il numero di vulnerabilità individuate (*discover*) e pubblicate a partire dal 2022.
18	L'organizzazione aderisce a codici formali di condotta e/o etici specifici per le attività di TLPT? Indicare i codici formali di condotta e/o etici a cui l'organizzazione aderisce.
Percezione del mercato dei servizi di TLPT	
19	Relativamente al mercato dei servizi di TLPT, esprimere il proprio grado di accordo con le seguenti affermazioni: a) La regolamentazione e l'adozione di framework pubblici e/o pubblico-privati ovvero quella di standard di settore favoriscono la crescita del mercato dei servizi di TLPT. b) La consapevolezza delle imprese sui rischi cyber favorisce la crescita del mercato dei servizi di TLPT. c) Lo sviluppo della tecnologia favorisce la crescita del mercato dei servizi di TLPT. d) L'utilizzo di soluzioni basate sull'intelligenza artificiale favorisce la crescita del mercato dei servizi di TLPT. e) La disponibilità limitata di personale con esperienza e competenze adeguate è uno dei principali problemi per lo sviluppo del mercato dei servizi di TLPT. f) Rispetto al budget economico assegnato dai clienti alle attività di cybersicurezza, il costo dei servizi di TLPT limita lo sviluppo del mercato dei servizi di TLPT.
20	Relativamente all'erogazione dei servizi di TLPT, esprimere il proprio grado di accordo con le seguenti affermazioni: a) Nell'erogazione dei servizi di TLPT l'adeguato trattamento dei dati riservati dei clienti è una delle principali difficoltà. b) Nell'erogazione dei servizi di TLPT il verificarsi di incidenti operativi è uno dei principali rischi. c) Nell'erogazione dei servizi di TLPT la relazione con il cliente è facilmente gestibile. d) Nell'erogazione dei servizi di TLPT gli obiettivi *(flags)* dell'attacco sono di facile individuazione. e) Nell'erogazione dei servizi di TLPT la gestione dei tempi del progetto concordati con il cliente è facile da rispettare. f) Nell'erogazione dei servizi di TLPT l'utilizzo di soluzioni basate sull'intelligenza artificiale aumenta la qualità o l'efficacia del servizio.

21	Come la vostra organizzazione giudica il livello di maturità del mercato dei servizi di TLPT?
22	Come la vostra organizzazione valuta rapporto tra domanda e offerta dei servizi di TLPT.

APPENDICE C – GLOSSARIO

Application security testing
Test di sicurezza in cui l'unità sottoposta a test è una singola applicazione.

Generic Threat Intelligence (GTI)
Attività di intelligence per l'analisi dello scenario di minaccia generale (ad es., per un intero settore) anche al di fuori del perimetro del singolo TLPT.

Penetration Testing (PT)
Una metodologia di test in cui i valutatori, utilizzando tutta la documentazione disponibile (ad esempio, progetto di sistema, codice sorgente, manuali) e lavorando sotto vincoli specifici, tentano di aggirare i presidi di sicurezza di un sistema informativo.
Fonte: FSB Cyber Lexicon

Red team report
Il Red team report è il documento redatto nella fase di chiusura delle attività di red teaming.

Red Teaming (RT)
Un test di sicurezza in cui operatori umani tentano di raggiungere obiettivi prefissati agendo come un attore della minaccia, senza, o con limitati, vincoli e senza alcuna notifica o avviso preventivo ai team di difesa (blue team) dell'organizzazione sottoposta al test.

Regulatory Technical Standards (RTS)
Atti delegati della Commissione UE che integrano o modificano determinati elementi non essenziali di un atto regolamentare di base e che richiedono la competenza di esperti in materia, generalmente redatti dalle Autorità di supervisione europee.

Security testing
Un processo strutturato che rivela se un sistema sottoposto a test presenta punti deboli che possono essere sfruttati per causare effetti indesiderati (ad esempio, manipolazione di dati, denial of service).

System security testing
Test di sicurezza in cui l'unità sottoposta a test è un insieme definito di componenti interconnessi.

Targeted Threat Intelligence (TTI)
La TTI fornisce una visione dettagliata sulla superficie di attacco dell'entità e sui suoi presìdi di difesa.
Fonte: Guida Nazionale TIBER-IT

Targeted Threat Intelligence (TTI) Report
Il TTI Report è un report di threat intelligence su misura per l'entità sottoposta al test. Lo stesso report TTI può essere aggiornato più volte durante un TLPT.

Threat Intelligence (TI)
Informazioni sulle minacce che sono state aggregate, trasformate, analizzate, interpretate o arricchite per fornire il contesto necessario ai processi decisionali.
Fonte: FSB Cyber Lexicon

Threat-Led Penetration Testing (TLPT) [46]

Un tentativo controllato di compromettere la resilienza cibernetica di un'entità simulando le tattiche, le tecniche e le procedure di attori della minaccia reali. Si basa sulla Targeted Threat Intelligence e si concentra sulle persone, i processi e la tecnologia di un'entità, con una conoscenza preliminare e un impatto minimo sull'operatività.

Fonte: FSB Cyber Lexicon

Vulnerability Assessment (VA)

Valutazione sistematica di un sistema informativo, dei suoi controlli e dei suoi processi, per determinare l'adeguatezza delle misure di sicurezza, identificare le carenze, fornire dati per prevedere l'efficacia delle misure di sicurezza proposte e confermare l'adeguatezza di tali misure dopo l'implementazione.

Fonte: FSB Cyber Lexicon

[46] Così definiti nell'art. 3 par. 17 del Regolamento DORA: "un quadro che imita le tattiche, le tecniche e le procedure di attori reali della minaccia che sono percepiti come minaccia informatica autentica, che consente di eseguire un test dei sistemi di produzione attivi e critici dell'entità finanziaria in maniera controllata, mirata e basata sull'analisi della minaccia (red team)".

Ultime pubblicazioni della collana
Mercati, infrastrutture, sistemi di pagamento

n. 26 Integrating DLTs with market infrastructures: analysis and proof-of-concept for secure DvP between TIPS and DLT platforms, *di Rosario La Rocca, Riccardo Mancini, Marco Benedetti, Matteo Caruso, Stefano Cossu, Giuseppe Galano, Simone Mancini, Gabriele Marcelli, Piero Martella, Matteo Nardelli, Ciro Oliviero* (Approfondimenti)

n. 27 Uso statistico e previsivo delle transazioni elettroniche di pagamento: la collaborazione Banca d'Italia-Istat, *di Guerino Ardizzi e Alessandra Righi* (Questioni istituzionali)

n. 28 TIPS: a zero-downtime platform powered by automation, *di Gianluca Caricato, Marco Capotosto, Silvio Orsini, Pietro Tiberi* (Approfondimenti)

n. 29 TARGET2 analytical tools for regulatory compliance, *di Marc Glowka, Alexander Müller, Livia Polo Friz, Sara Testi, Massimo Valentini, Stefano Vespucci* (Questioni istituzionali)

n. 30 The security of retail payment instruments: evidence from supervisory data, *di Massimiliano Cologgi* (Approfondimenti)

n. 31 Open Banking in the payment system: infrastructural evolution, innovation and security, supervisory and oversight practices, *di Roberto Pellitteri, Ravenio Parrini, Carlo Cafarotti, Benedetto Andrea De Vendictis* (Questioni istituzionali)

n. 32 Banks' liquidity transformation rate: determinants and impact on lending, *di Raffaele Lenzi, Stefano Nobili, Filippo Perazzoli, Rosario Romeo* (Approfondimenti)

n. 33 Investor behavior under market stress: evidence from the Italian sovereign bond market, *di Onofrio Panzarino* (Approfondimenti)

n. 34 Reti neurali siamesi per la rilevazione dei difetti di stampa delle banconote, *di Katia Boria, Andrea Luciani, Sabina Marchetti, Marco Viticoli* (Approfondimenti)

n. 35 Quantum safe payment systems, *di Elena Bucciol, Pietro Tiberi*

n. 36 Investigating the determinants of corporate bond credit spreads in the euro area, *di Simone Letta, Pasquale Mirante*

n. 37 Smart Derivative Contracts in DatalogMTL, *di Andrea Colombo, Luigi Bellomarini, Stefano Ceri, Eleonora Laurenza*

n. 38 Making it through the (crypto) winter: facts, figures and policy issues, *di Guerino Ardizzi, Marco Bevilacqua, Emanuela Cerrato, Alberto Di Iorio*

n. 39 Il sistema per lo scambio delle quote di emissione dell'UE (ETS UE), *di Mauro Bufano, Fabio Capasso, Johnny Di Giampaolo, Nicola Pellegrini*

n. 40 La migrazione delle banconote e la stima della circolazione nei paesi dell'area dell'euro: il caso italiano, *di Claudio Doria, Gianluca Maddaloni, Giuseppina Marocchi, Ferdinando Sasso, Luca Serrai, Simonetta Zappa*

n. 41 Assessing credit risk sensitivity to climate and energy shocks, *di Stefano Di Virgilio, Ivan Faiella, Alessandro Mistretta, Simone Narizzano*

n. 42 Report on the payment attitudes of consumers in italy: results from the ECB SPACE 2022 survey, *di Gabriele Coletti, Alberto Di Iorio, Emanuele Pimpini, Giorgia Rocco*

n. 43 A service architecture for an enhanced Cyber Threat Intelligence capability and its value for the cyber resilience of Financial Market Infrastructures, *di Giuseppe Amato, Simone Ciccarone, Pasquale Digregorio, Giuseppe Natalucci*

n. 44 Fine-tuning large language models for financial markets via ontological reasoning, *di Teodoro Baldazzi, Luigi Bellomarini, Stefano Ceri, Andrea Colombo, Andrea Gentili, Emanuel Sallinger*

n. 45 La sostenibilità nelle assemblee societarie in Francia, Germania e Italia, *di Tiziana De Stefano, Giuseppe Buscemi, Marco Fanari*

n. 46 Money market rate stabilization systems over the last 20 years: the role of the minimum reserve requirement, *di Patrizia Ceccacci, Barbara Mazzetta, Stefano Nobili, Filippo Perazzoli, Mattia Persico*

n. 47 I fornitori di tecnologia nel sistema dei pagamenti: evoluzione di mercato e quadro normativo, *di Emanuela Cerrato, Enrica Detto, Daniele Natalizi, Federico Semorile, Fabio Zuffranieri*

n. 48 The fundamental role of the repo market and central clearing, *di Cristina Di Luigi, Antonio Perrella, Alessio Ruggieri*

n. 49 From Public to Internal Capital Markets: The Effects of Affiliated IPOs on Group Firms, *di Luana Zaccaria, Simone Narizzano, Francesco Savino, Antonio Scalia*

n. 50 Byzantine Fault Tolerant consensus with confidential quorum certificate for a Central Bank DLT, *di Marco Benedetti, Francesco De Sclavis, Marco Favorito, Giuseppe Galano, Sara Giammusso, Antonio Muci, Matteo Nardelli*

n. 51 Environmental data and scores: lost in translation, *di Enrico Bernardini, Marco Fanari, Enrico Foscolo, Francesco Ruggiero*

n. 52 How important are ESG factors for banks' cost of debt? An empirical investigation, *di Stefano Nobili, Mattia Persico, Rosario Romeo*

n. 53 The Bank of Italy's statistical model for the credit assessment of non-financial firms, *di Simone Narizzano, Marco Orlandi, Antonio Scalia*

n. 54 The revision of PSD2 and the interplay with MiCAR in the rules governing payment services: evolution or revolution?, *di Mattia Suardi*

n. 55 Rating the Raters. A Central Bank Perspective, *di Francesco Columba, Federica Orsini, Stefano Tranquillo*

n. 56 A general framework to assess the smooth implementation of monetary policy: an application to the introduction of the digital euro, *di Annalisa De Nicola, Michelina Lo Russo*

n. 57 The German and Italian Government Bond Markets: The Role of Banks versus Non-Banks. A joint study by Banca d'Italia and Bundesbank, *di Puriya Abbassi, Michele Leonardo Bianchi, Daniela Della Gatta, Raffaele Gallo, Hanna Gohlke, Daniel Krause, Arianna Miglietta, Luca Moller, Jens Orben, Onofrio Panzarino, Dario Ruzzi, Willy Scherrieble, Michael Schmidt*

n. 58 Chat Bankman-Fried? An Exploration of LLM Alignment in Finance, *di Claudia Biancotti, Carolina Camassa, Andrea Coletta, Oliver Giudice, Aldo Glielmo*

n. 59 Modelling transition risk-adjusted probability of default, *di Manuel Cugliari, Alessandra Iannamorelli, Federica Vassalli*

n. 60 The use of Banca d'Italia's credit assessment system for Italian non-financial firms within the Eurosystem's collateral framework, *di Stefano Di Virgilio, Alessandra Iannamorelli, Francesco Monterisi, Simone Narizzano*

n. 61 Metodologia di classificazione del Fintech, *di Alessandro Lentini, Daniela Elena Munteanu, Fabrizio Zennaro*

n. 62 The Rise of Climate Risks: Evidence from Expected Default Frequencies for Firms, *di Matilde Faralli, Francesco Ruggiero*