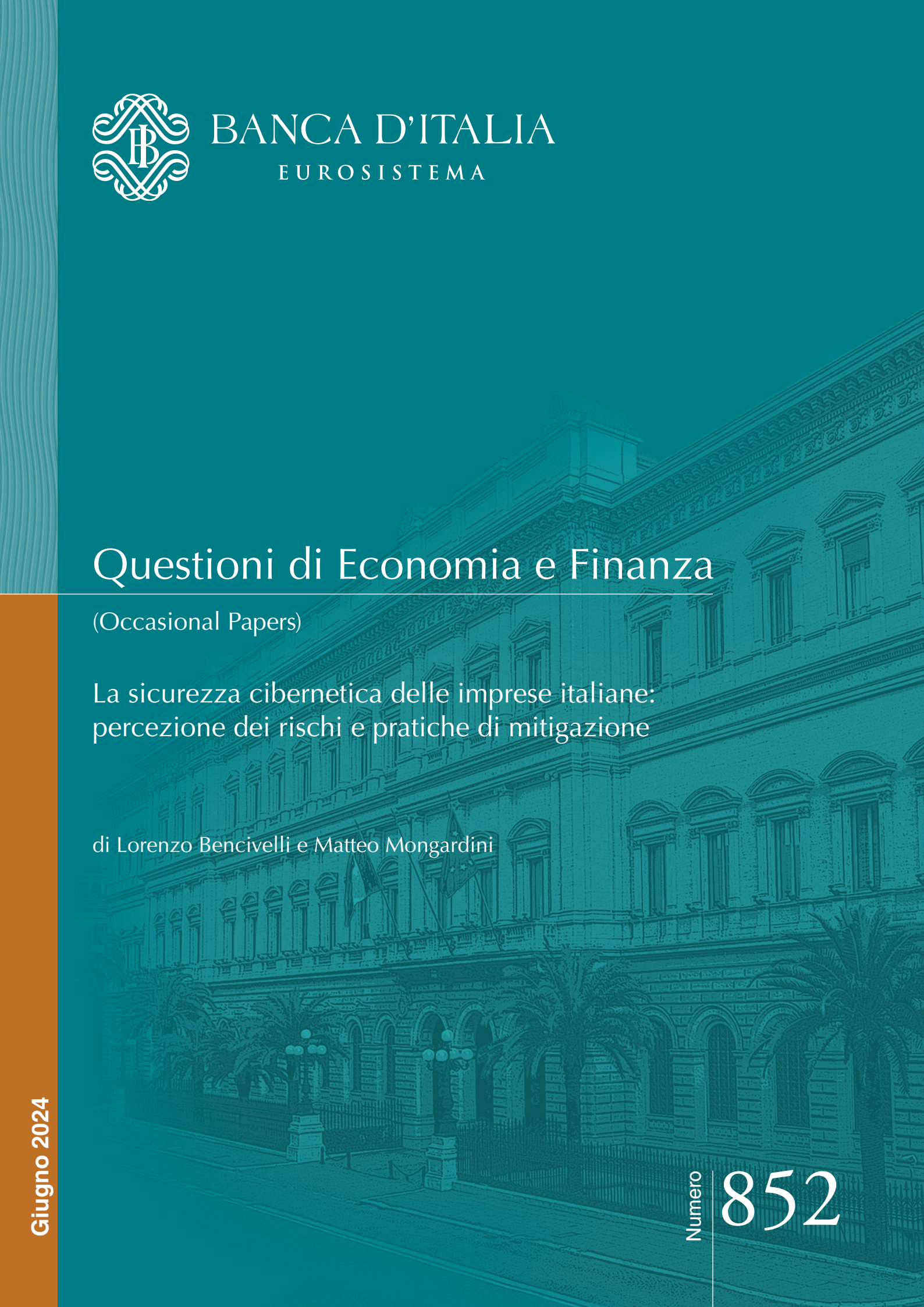
BANCA D'ITALIA
EUROSISTEMA

Questioni di Economia e Finanza

(Occasional Papers)

La sicurezza cibernetica delle imprese italiane: percezione dei rischi e pratiche di mitigazione

di Lorenzo Bencivelli e Matteo Mongardini



Numero 852

Giugno 2024

BANCA D'ITALIA
EUROSISTEMA

Questioni di Economia e Finanza

(Occasional Papers)

La sicurezza cibernetica delle imprese italiane: percezione dei rischi e pratiche di mitigazione

di Lorenzo Bencivelli e Matteo Mongardini

Numero 852 – Giugno 2024

La serie Questioni di economia e finanza *ha la finalità di presentare studi e documentazione su aspetti rilevanti per i compiti istituzionali della Banca d'Italia e dell'Eurosistema. Le* Questioni di economia e finanza *si affiancano ai* Temi di discussione *volti a fornire contributi originali per la ricerca economica.*

La serie comprende lavori realizzati all'interno della Banca, talvolta in collaborazione con l'Eurosistema o con altre Istituzioni. I lavori pubblicati riflettono esclusivamente le opinioni degli autori, senza impegnare la responsabilità delle Istituzioni di appartenenza.

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

ISSN 1972-6643 (online)

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

LA SICUREZZA CIBERNETICA DELLE IMPRESE ITALIANE: PERCEZIONE DEI RISCHI E PRATICHE DI MITIGAZIONE

di Lorenzo Bencivelli* e Matteo Mongardini*

Sommario

Lo studio valuta il livello di consapevolezza delle imprese circa i rischi cibernetici e la loro capacità di adottare strategie di mitigazione sulla base delle evidenze raccolte con le edizioni del 2016 e del 2022 dell'*Indagine sulle imprese industriali e dei servizi* della Banca d'Italia. Quasi il 90 per cento delle imprese è consapevole della possibilità di subire un attacco informatico, cui però non sempre corrisponde un adeguato impegno finanziario per fronteggiarne i rischi. Le imprese che in passato hanno subito un attacco mostrano una maggiore percezione del rischio a cui si associa una più elevata spesa in prevenzione. Le imprese più piccole e quelle del Mezzogiorno risultano meno consapevoli dei rischi cibernetici.

Classificazione JEL: C83, F50, L60, L80, M15, O33.

Parole chiave: imprese, sicurezza cibernetica, percezione del rischio.

DOI: 10.32057/0.QEF.2024.0852

* Banca d'Italia, Dipartimento Economia e Statistica.

1. Introduzione[1]

La minaccia cibernetica è per sua natura mutevole e richiede un presidio costante e flessibile. Il rapporto al Parlamento sul 2022 del Dipartimento per le Informazioni e la Sicurezza[2] registra ad esempio un sostanziale cambio di orientamento di questa minaccia rispetto agli ultimi cinque anni: nel 2022 gli attacchi cibernetici si sono concentrati su obiettivi privati, mentre negli anni precedenti avevano preso di mira in prevalenza infrastrutture a controllo pubblico. Nel settore privato le imprese italiane sono bersagli potenziali poiché posseggono e custodiscono dati sensibili relativi ai loro clienti, alle proprie dotazioni, a brevetti e altre attività immateriali. Impossessarsi di tale patrimonio informativo o codificarlo con chiave crittografica per condizionarne la liberazione al pagamento di un riscatto (c.d. *ransomware*) costituiscono delle possibilità di guadagno per i gruppi criminali dediti a questa attività.

La preparazione delle aziende verso il rischio informatico è ancora scarsamente documentata e le informazioni disponibili sono per lo più diffuse da società di consulenza che hanno un interesse commerciale nella materia. Nell'Indagine sulle Imprese Industriali e dei Servizi sul 2016[3] (INVIND-16) è stato incluso per la prima volta un blocco di domande sulla sicurezza cibernetica. Le domande si concentrarono sui presidi hardware, software e umani a tutela della sicurezza cibernetica, sulla spesa sostenuta per l'acquisizione di tali presidi e su eventuali danni verificatisi a seguito di attacchi cibernetici. Nell'edizione della stessa indagine relativa al 2022[4] (INVIND-22), è stata inserita una sezione monografica sul tema della cybersicurezza con domande simili a quelle dell'edizione sul 2016[5]. A differenza che nel 2022, nel 2016 non era presente una domanda sulla percezione del rischio ma è comunque possibile effettuare delle valutazioni a partire dalla numerosità e sofisticazione degli strumenti che le imprese intervistate hanno dichiarato nella propria dotazione.

I risultati dell'indagine sul 2016 sono stati descritti in dettaglio da Biancotti (2017a e 2017b), che ha delineato un quadro caratterizzato da un numero piuttosto consistente di imprese che dichiaravano di aver subito attacchi, a seguito dei quali solo alcune avevano maturato una certa consapevolezza del

[1] Gli autori ringraziano per i preziosi commenti e la proficua collaborazione C. Biancotti, S. Marchetti, A. Borin e M. Bottone, V. Vacca, A. Neri, C. Rondinelli e tutti i membri della segreteria del Comitato per la Sicurezza Cibernetica della Banca d'Italia che ha dato indicazione di procedere con questo progetto. Le opinioni espresse sono personali e non riflettono necessariamente la posizione della Banca d'Italia.

[2] Per maggiori informazioni si veda il documento completo sul sito della Sistema di informazione per la sicurezza della Repubblica.

[3] L'indagine è svolta dalla Banca d'Italia presso un campione di oltre 4.000 imprese italiane dell'industria in senso stretto e dei servizi privati non finanziari con almeno 20 addetti. Per maggiori informazioni sulla metodologia si può consultare la nota "*Metodi e fonti: note metodologiche*" della pubblicazione.

[4] In questa edizione la sezione monografica sulla cybersicurezza è stata sottoposta a solo metà del campione, ma grazie al sistema di pesi è possibile confrontare le due indagini.

[5] Nelle rilevazioni relative agli anni tra 2017 e 2020 è stata mantenuta la sola domanda sull'occorrenza di un attacco cibernetico.

rischio cibernetico. Inoltre, anche a fronte di tale consapevolezza, la spesa per il presidio delle funzioni aziendali sensibili verso queste minacce era rimasta su livelli piuttosto contenuti.

Questa nota riporta i principali risultati sul tema della cybersicurezza dell'indagine sul 2022, anche nel confronto con il quadro emerso nel 2016 per tracciare l'evoluzione delle due variabili di consapevolezza e intervento nei sei anni e identificando eventuali fattori che potrebbero avere inciso sul diverso atteggiamento delle imprese nei confronti del fenomeno.

2. Consapevolezza dei rischi e incidenza del problema

2.1 Consapevolezza dei rischi

Per valutare la consapevolezza del rischio da parte delle imprese la domanda, formulata tenendo conto della possibile reticenza nell'ammettere la propria vulnerabilità, è stata posta come segue:

Domanda 1

Quanto ritenete probabile che un'azienda simile alla Vostra (per dimensione e settore di attività) possa subire attacchi cibernetici?

(a) per nulla probabile *(b) poco probabile* *(c) molto probabile*

La percentuale di imprese che ritengono per nulla probabile che un attacco cibernetico possa interessare un'impresa con le loro stesse caratteristiche è pari all'11,6 per cento (Tav. 1); tale percentuale sale al 14,2 per le imprese con meno di 50 addetti e al 17,2 per quelle del sud e delle isole. Come nella rilevazione sul 2016, l'occorrenza di un evento potenzialmente distruttivo sui propri sistemi digitali rimane un fattore significativo nella maturazione della consapevolezza del rischio: la quasi totalità delle aziende che sono state oggetto di un attacco cyber (il 23,4 per cento delle imprese ha dichiarato almeno un attacco nell'ultimo quinquennio)[6] ritengono di essere soggette a un qualche rischio. Al netto di alcune eccezioni, la percezione del rischio non varia in maniera significativa tra settori.

[6] Come vedremo in seguito, alle aziende è stato chiesto se sono state vittima di attacco cibernetico nell'ultimo quinquennio.

Tav. 1: Quanto è probabile che azienda simile alla propria possa subire attacchi cibernetici
(*Percezione del rischio per caratteristiche individuali delle imprese; valori percentuali*)

	Totale imprese			Non ha subito attacchi			Ha subito attacchi			
	(1) Per nulla	(2) Poco	(3) Molto	(4) Per nulla	(5) Poco	(6) Molto	(7) Per nulla	(8) Poco	(9) Molto	(10) Numero risposte
Area geografica										
Centro Nord	10,3	68,0	21,7	13,6	73,9	12,5	0,1	49,8	50,1	1.108
Sud e Isole	17,2	64,0	18,8	20,6	67,8	11,6	1,8	47,2	51,0	630
Numero di addetti										
20 - 49	14,2	69,8	16,1	17,6	72,6	9,9	0,2	58,2	41,6	560
50 e oltre	6,6	62,4	31,0	9,2	73,1	17,8	0,7	38,6	60,8	1.178
Attività economica										
Tessili, abbigl., pelli, calzature	23,7	65,9	10,4	30,0	63,1	7,0	0,8	76,1	23,1	109
Chimica, gomma e plastica	4,8	70,5	24,7	5,4	73,8	20,8	2,4	55,0	42,7	147
Metalmeccanica	10,6	70,0	19,5	13,5	76,1	10,4	.	48,3	51,7	464
Altre manifatturiere	14,0	63,4	22,6	17,6	67,7	14,7	.	46,6	53,4	366
Energetiche ed estrattive	10,2	69,2	20,5	18,4	75,4	6,2	.	61,5	38,5	82
Commercio, alberghi e ristorazione	11,9	70,4	17,7	14,1	73,8	12,1	1,4	54,4	44,2	267
Trasporti, magazz. e comunicazioni	7,5	65,3	27,2	10,3	76,6	13,1	.	35,3	64,7	194
Altri servizi a imprese e famiglie	12,2	61,7	26,2	18,3	68,5	13,2	.	47,9	52,1	109
Totale industria in s.s e servizi	**11,6**	**67,3**	**21,2**	**15,0**	**72,7**	**12,3**	**0,4**	**49,4**	**50,2**	**1.738**

Note: statistiche ponderate per i pesi di riporto al numero delle imprese dell'universo.

Conclusioni simili possono essere tratte da un'analisi multivariata (Tav. 2), in cui si considera anche il valore aggiunto per addetto come *proxy* per il livello di sofisticazione delle imprese: è verosimile, infatti, che aziende più produttive siano anche più sensibili al rischio cibernetico.

L'essere stato oggetto di un attacco cibernetico si conferma un fattore chiave nello spiegare il rischio dichiarato, indipendentemente dalle caratteristiche delle imprese (si noti l'invarianza del coefficiente tra le specificazioni 1 e 6). Come atteso, il fatturato per addetto risulta positivamente correlato con il rischio dichiarato, così come la dimensione d'impresa. D'altra parte, la collocazione dell'impresa nel meridione riporta un coefficiente significativo solo se la si considera disgiuntamente dalla dimensione, suggerendo che il rischio dichiarato sia legato soprattutto alla dimensione dell'impresa più che all'area geografica in cui essa opera (e la presenza di piccole e medie imprese è maggiore nel sud d'Italia)[7].

[7] Utilizzando una disaggregazione più sottile (non riportata qui) le imprese del Nord-Est sembrano dichiarare un rischio più alto rispetto alle altre del Centro-Nord.

Infine, come già emerso dall'analisi descrittiva, le differenze settoriali sono sostanzialmente poco o non significative e solo l'appartenenza al settore tessile e a quello energetico/estrattivo si associa a una riduzione del rischio dichiarato.

Tav. 2: Analisi di regressione non lineare (ordered logit): rischio cibernetico dichiarato

	(1)	(2)	(3)	(4)	(5)	(6)
Attacco	2,052***					2,202***
	(0,212)					(0,218)
Valore aggiunto per addetto		0,539*				0,931***
		(0,315)				(0,283)
Sud e isole			-0,345**			-0,005
			(0,171)			(0,222)
50 - 200 addetti				0,680***		0,713***
				(0,179)		(0,190)
Oltre 200 addetti				1,370***		1,271***
				(0,191)		(0,229)
Tessili, abbigl., pelli, calzature					-0,841**	-1,269***
					(0,397)	(0,484)
Chimica, gomma e plastica					0,377	0,253
					(0,285)	(0,414)
Metalmeccanica					-0,0684	-0,064
					(0,239)	(0,300)
Energetiche ed estrattive					0,0803	-0,980**
					(0,324)	(0,416)
Commercio, alberghi e ristorazione					-0,157	-0,421
					(0,284)	(0,329)
Trasporti, magazz. e comunicazioni					0,391	0,398
					(0,273)	(0,336)
Altri servizi a imprese e famiglie					0,170	-0,014
					(0,355)	(0,422)
Osservazioni	1.738	1.483	1.778	1.778	1.778	1.465

Note: Logit ordinale; la variabile dipendente è data dalle risposte alla Domanda 1 e prende valore 0 (nessun rischio), 1 (basso rischio) e 2 (alto rischio). Standard error robusti in parentesi. *** p<0.01, ** p<0.05, * p<0.

I risultati presentati finora assumono che le aziende siano soggette allo stesso livello di minaccia cibernetica.

La domanda 1 si riferisce al rischio percepito dalle imprese che dipende, oltre che dalla sensibilità dell'impresa verso questi temi, dalla componente ambientale (ovvero l'operare in settori più rischiosi) e dal perimetro di esposizione[8] dell'impresa stessa. Il primo fattore è catturato da una variabile *dummy* che assume valore 1 per i settori che hanno subito più attacchi della media della popolazione (in Tav. 3 il valore dell'indicatore di rischiosità settoriale). La quota di investimenti in tecnologie avanzate sul totale

[8] Per "superficie di attacco" o "perimetro di esposizione" si intende l'insieme dei possibili punti di attacco di una rete informatica aziendale, ovvero tutti gli snodi che possono essere raggiunti da internet come il sito e i server aziendali o le infrastrutture remote come le risorse memorizzate all'interno di servizi di cloud. In un'accezione più recente, in ragione dello sviluppo del lavoro a distanza, anche i dipendenti e le loro dotazioni personali sono considerati facenti parte della superficie d'attacco.

può aiutare a catturare la dimensione del rischio specifica della singola impresa poiché con la maggiore dotazione di asset tecnologici crescono anche la superficie di esposizione (ma sconnessa dalla sua percezione , rischio oggettivo idiosincratico)[9]. Sebbene la definizione impiegata in INVIND per il concetto di "tecnologie avanzate" sia piuttosto ampia (include per esempio l'impiego di attività che non implicano necessariamente un aumento dell'esposizione al rischio cyber), possiamo assumere che un ampio ricorso a questo tipo di investimenti possa aumentare la superficie d'attacco e, quindi, il patrimonio che l'impresa dovrà proteggere per mantenere l'efficienza operativa. Tuttavia, una quota elevata di investimenti in tali tecnologie può anche indicare l'acquisizione e il continuo aggiornamento di strumenti dotati di presidi di sicurezza in grado di offrire una difesa robusta verso possibili attacchi. Non abbiamo strumenti per controllare per tale possibile fonte di endogeneità, pertanto questa limitazione va considerata nell'interpretazione dei risultati. Infine, la quota di fatturato all'export controlla per il grado di esposizione ai mercati internazionali.

Tav. 3: Indicatore di rischio settoriale

	(1) Quota su popolazione	(2) Frequenza attacchi	(3) Indicatore di rischio
Tessili, abbigl., pelli, calzature	5,77	23,46	0
Chimica, gomma e plastica	4,67	17,81	0
Metalmeccanica	21,90	23,37	0
Altre manifatturiere	11,49	22,40	0
Energetiche ed estrattive	2,66	46,10	1
Commercio, alberghi e ristorazione	25,39	19,14	0
Trasporti, magazz. e comunicazioni	9,71	24,11	0
Altri servizi a imprese e famiglie	5,60	35,26	1

Note: frequenza di aziende che hanno subito almeno un attacco nel quinquennio precedente e valore dell'indicatore di rischio.

In Tav. 4 sono riportate le stime dei coefficienti di varie formulazioni del logit ordinale. In linea di massima, i coefficienti statisticamente significativi nelle specificazioni più parsimoniose risultano tali anche in quella estesa (con valori stimati molto simili), suggerendo che ciascuna variabile esplicativa colga una dimensione ben distinta dalle altre. L'unica eccezione è rappresentata dalla variabile "Attacco" (l'impresa dichiara di aver subito almeno un attacco cibernetico nell'ultimo quinquennio, significativa in tutte le specificazioni) che risente dell'interazione significativa con gli investimenti tecnologici.[10] Come ipotizzato in precedenza, gli asset tecnologici di nuova acquisizione sono di sovente dotati dal fornitore di presidi di sicurezza, mitigando così l'effetto dell'utilizzo di tecnologie

[9] Per esigenze di calcolo, la variabile è stata portata da 5 a tre categorie: "zero investimenti tecnologici", "bassi investimenti tecnologici" fino al 5 per cento del totale e "alti investimenti tecnologici" per quote superiori.
[10] Le due variabili *dummy* sono definite sulla base della risposta alla Domanda 1: "rischio medio" prende valore 1 per tutte le imprese che hanno risposto di ritenere "poco probabile" un attacco cibernetico; "rischio alto" prende valore 1 per tutte le imprese che hanno risposto "molto probabile".

maggiormente esposte a possibili attacchi e dall'esserne già stato oggetto. La rischiosità del settore non apporta un contenuto esplicativo significativo così come la sua interazione con l'occorrenza di un attacco informatico. Questa informazione è coerente con quanto osservato in Tav. 1 e Tav. 3, ovvero una certa uniformità del rischio dichiarato tra settori, sia che siano stati oggetto di un numero di attacchi superiore o inferiore rispetto alla media.

Tav. 4: Analisi di regressione non lineare (ordered logit): rischio cibernetico dichiarato

	(1)	(2)	(3)	(4)	(5)
Attacco	2,197***	2,209***	3,212***	2,689***	3,726***
	(0,221)	(0,221)	(0,425)	(0,418)	(0,567)
Valore aggiunto per addetto	0,950***	0,932***	0,972***	0,957***	1,004***
	(0,285)	(0,284)	(0,308)	(0,295)	(0,322)
Settore a rischio		-0,0013			-0,0681
		(0,506)			(0,545)
Attacco * settore a rischio		-0,0307			-0,387
		(0,621)			(0,653)
Bassi investimenti tecnologici			0,879***		0,885***
			(0,323)		(0,328)
Alti investimenti tecnologici			0,791***		0,759***
			(0,277)		(0,277)
Attacco * bassi investimenti tecnologici			-1,617***		-1,589***
			(0,566)		(0,570)
Attacco * alti investimenti tecnologici			-1,622***		-1,483***
			(0,493)		(0,486)
Basso fatturato all'export				0,349	0,318
				(0,282)	(0,289)
Alto fatturato all'export				-0,138	-0,202
				(0,392)	(0,398)
Attacco * basso fatturato all'export				-0,787	-0,843*
				(0,503)	(0,509)
Attacco * alto fatturato all'export				-0,711	-0,652
				(0,496)	(0,551)
Controlli	si	si	si	si	si
Osservazioni	1.430	1.465	1.430	1.465	1.430

Note: Logit ordinale; la variabile dipendente prende tre valori: 0 ("zero rischio"), 1 ("basso rischio") e 2 ("alto rischio"). I controlli includono dummy di settore, area geografica di residenza ("centro nord" e "sud e isole") e di dimensione ("piccola", "media" o "grande"). Standard error robusti in parentesi. *** p<0.01, ** p<0.05, * p<0.1.

Gli investimenti tecnologici apportano un contributo informativo significativo e di segno positivo, suggerendo che la dotazione di tecnologie avanzate è vista dalle imprese come un fattore di rischio soggettivo. Tuttavia, la sua interazione con l'occorrenza di un attacco nell'ultimo quinquennio, significativa ma con un coefficiente negativo, suggerisce che le imprese potrebbero avere fatto esperienza degli attacchi subiti e aver investito una quota di risorse nella mitigazione del rischio informatico. L'esposizione ai mercati internazionali non fornisce un contributo rilevante.

2.2 Rilevanza degli attacchi

Per avere una stima della rilevanza numerica degli attacchi cibernetici e della loro pervasività, l'indagine ha proposto alle aziende la seguente domanda:

Domanda 2

Negli ultimi 5 anni, la Vostra azienda ha subito un danno patrimoniale a seguito di un attacco cibernetico?

(a) Non ha subito attacchi *(b) Ha subito attacchi, ma senza danni* *(c) Sì*

Tav. 5: Danni patrimoniali da attacco cibernetico negli ultimi 5 anni
(*quota percentuale di imprese; pesati per rimando all'universo campionario e al totale del fatturato*)

	Quota imprese			Quota fatturato			
	(1)	(2)	(3)	(4)	(5)	(6)	(7)
	No, perché non ha subito attacchi	No, ha subito attacchi ma senza danni	Sì	No, perché non ha subito attacchi	No, ha subito attacchi ma senza danni	Sì	Numero risposte
Area geografica							
Centro Nord	75,5	19,9	4,7	52,3	42,4	5,4	1.116
Sud e Isole	81,6	12,8	5,6	70,1	23,4	6,5	633
Numero di addetti							
20 - 49	80,5	15,2	4,3	77,3	18,9	3,8	562
50 e oltre	69,2	25,0	5,8	47,3	46,8	6,0	1.187
Totale industria in s.s e servizi	**76,6**	**18,5**	**4,8**	**54,0**	**40,5**	**5,5**	**1.749**

Note: Statistiche ponderate per i pesi di riporto al numero delle imprese dell'universo per quota imprese e al totale del fatturato per quota fatturato.

Poco meno di un quarto delle imprese dichiara di aver subito attacchi nell'ultimo quinquennio; questa quota scende al 18 per cento tra le imprese del meridione e delle isole (Tav. 5). Tra i vari settori, l'unica differenza sostanziale è fornita dal comparto energetico, dove quasi un'azienda su due dichiara di essere stata oggetto di attacco, per lo più senza danni. La quota di imprese che dichiarano di non aver subito attacchi decresce all'aumentare della dimensione aziendale. L'aumento degli incidenti riportati fra le imprese più grandi è particolarmente evidente se si guarda alla quota di fatturato coinvolto: le imprese interessate dagli attacchi cibernetici contano infatti per il 46 per cento del fatturato pur rappresentando meno di un quarto delle imprese nella popolazione. Di contro, le quote di imprese e di fatturato sono simili (intorno al 5 per cento) quando si considerano le imprese che hanno riportato danni patrimoniali a seguito degli attacchi registrati. Ciò suggerisce che le imprese di maggiori dimensioni dispongono di migliori strumenti di sicurezza informatica rispetto a quelle medio-piccole.

Il più alto numero di attacchi alle imprese di maggiore dimensione potrebbe dipendere dalla loro maggiore capacità di registrare e documentare l'occorrenza di una violazione, rendendo di fatto la statistica più attendibile rispetto a quella delle piccole imprese, dotate di sistemi di rilevazione e

reporting meno avanzati. Tuttavia, la maggiore visibilità delle grandi imprese e il più alto rendimento atteso dall'agente malevolo a seguito di un eventuale attacco[11] potrebbero giustificare una loro maggiore esposizione rispetto alle aziende di minore dimensione. Allo stesso tempo, la presenza di una struttura organizzativa meglio equipaggiata spiegherebbe i minori danni patrimoniali a fronte del maggior numero di attacchi.

I risultati vanno letti tenendo presente che l'indagine potrebbe sottostimare la vera entità del fenomeno per almeno due ragioni: *i)* alcuni attacchi cibernetici non sono rilevati neppure dalle imprese che ne sono vittime; *ii*) le imprese possono essere riluttanti a riportare l'occorrenza di incidenti cibernetici o la reale dimensione degli eventuali danni patrimoniali per motivi reputazionali.

Tav. 6: Danni patrimoniali da attacco cibernetico: confronto tra le rilevazioni del 2016 e 2022
(*quota percentuale di imprese; pesati per rimando all'universo campionario e al totale del fatturato*)

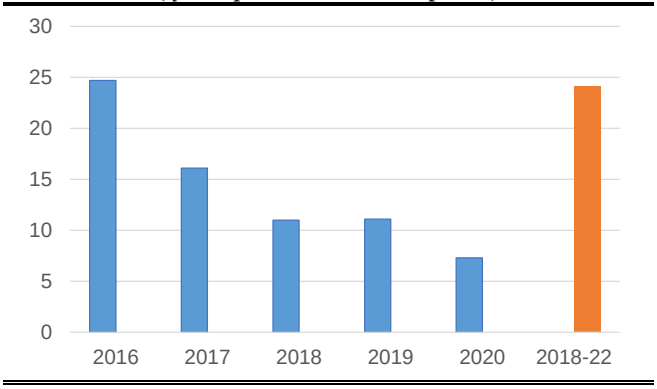
	(1) No, perché non ha subito attacchi	(2) No, ha subito attacchi ma senza danni	(3) Sì	(4) Numero risposte
Anno di rilevazione				
2016	76,8	7,1	16,0	3.548
2022	76,6	18,5	4,8	1.749
Attacco cibernetico nel 2016		**Rilevazione 2022**		
No	81,2	14,3	4,5	719
Sì	60,5	32,0	7,4	322

Note: statistiche ponderate per i pesi di riporto al numero delle imprese dell'universo. Raffronto con la rilevazione del 2016, con panel di imprese che hanno risposto ad entrambe le indagini.

È possibile fare un confronto con la rilevazione sul 2016, pur tenendo conto della diversa struttura delle domande nelle due rilevazioni: nel 2016 la domanda si riferiva esclusivamente a quanto successo nell'anno precedente, mentre in quella sul 2022 il periodo considerato è l'ultimo quinquennio (Tav. 6, pannello superiore)[12].

[11] Aziende dal fatturato più alto tendono a essere depositarie di un numero maggiore di informazioni sensibili, per esempio in ragione di una clientela più numerosa e variegata o di un perimetro di business più ampio ed eterogeneo. Inoltre, attacchi di successo a queste imprese possono avere una visibilità decisamente maggiore, aspetto che li rende più interessanti agli occhi di attori malevoli ispirati da motivi ideologici.
[12] Nella rilevazione sul 2016, inoltre, la domanda sull'occorrenza di un incidente di natura cibernetica era separata da quella che chiedeva di quantificare i danni che ne erano derivati mentre nel 2022 le due sono state accorpate nell'interesse della parsimonia.

Fig. 1: Numero di aziende che hanno subito almeno un attacco cibernetico
(*quota percentuale di imprese*)



Note: statistiche ponderate per i pesi di riporto al numero delle imprese dell'universo.

La domanda sull'occorrenza di un attacco è stata mantenuta fino alla rilevazione relativa al 2020: la frequenza degli episodi di attacchi cibernetici appare in riduzione, dal 25 al 7 per cento (Fig. 1)[13]. Il dato di INVIND-22 sembra coerente con tale tendenza se lo si distribuisce lungo il periodo considerato nella domanda.

Inoltre, a fronte di una simile percentuale di attacchi dichiarati, scende quella di coloro che ne hanno subito un danno patrimoniale, suggerendo una maggiore preparazione delle imprese di fronte a questa eventualità.

Analizzando i dati sulle imprese che hanno partecipato ad entrambe le rilevazioni (compente panel) si evince che quelle che avevano segnalato un attacco nel 2016 ne hanno subito almeno uno nel quinquennio successivo in proporzione superiore a quelle che non ne avevano subiti nel 2016. Una quota maggiore si riscontra anche negli attacchi con danni patrimoniali (Tav. 6, pannello inferiore). Questa evidenza suggerisce che numerose imprese sarebbero rimaste esposte ad attacchi cibernetici o che i rimedi impiegati potrebbero essersi rivelati insufficienti; un'ulteriore interpretazione è che grazie all'esperienza acquisita, queste imprese hanno una maggiore capacità di identificazione degli attacchi e/o una minore riluttanza a riferirne in sede di rilevazione.

3. Livello, dinamica e destinazione della spesa

In questa sezione si valuterà se le imprese trasformano la percezione o la consapevolezza del rischio in azioni concrete, come aumentare la spesa o dotarsi di una funzione dedicata alla sicurezza cibernetica.

Le evidenze raccolte si basano sulle risposte alla seguente domanda:

Domanda 3

Nel complesso del biennio 2021-2022, approssimativamente quale spesa ha sostenuto la Vostra azienda per tutelarsi dal rischio di attacchi cibernetici?

(a) Nessuna spesa *(b) Inferiore a € 5.000* *(c) Tra € 5.001 e € 10.000*
(d) Tra € 10.001 e € 50.000 *(e) Tra € 50.001 e € 200.000* *(f) Oltre € 200.000*

13 Tra il 2016 e il 2020 la domanda misurava gli attacchi nell'anno di osservazione, nell'ultima versione, è stata reintrodotta la domanda ma con riferimento al quinquennio precedente.

Si è ricorso a un'analisi di regressione non lineare (*ordered logit*) per isolare le caratteristiche individuali associate a una maggiore spesa per la sicurezza cibernetica (Tav. 7). Tra le variabili indipendenti, $RischioDichiarato_i$ e $Attacco_i$ sono state descritte nel paragrafo precedente. Aziende con un livello maggiore di investimenti in tecnologie avanzate, *InvestimentiTec*, possono aver sviluppato una sensibilità maggiore verso la sicurezza cibernetica poiché vedono esposta una quota maggiore delle proprie attività a possibili incidenti di questo tipo[14].

Tav. 7: Analisi di regressione non lineare (ordered logit): spesa per sicurezza cibernetica

	(1)	(2)	(3)	(4)	(5)	(6)
Attacco		1,479***	0,985		1,410***	0,703
		(0,210)	(0,726)		(0,207)	(0,775)
Basso rischio dichiarato	1,597***		1,624***	1,502***		1,506***
	(0,264)		(0,261)	(0,282)		(0,278)
Alto rischio dichiarato	3,554***		3,264***	3,429***		3,187***
	(0,305)		(0,340)	(0,322)		(0,365)
Attacco * basso rischio			-0,270			-0,00310
			(0,783)			(0,827)
Attacco * alto rischio			-0,0667			0,0694
			(0,784)			(0,836)
Bassi investimenti tec.	1,119***	0,934***	1,036***	1,054***	0,882***	0,983***
	(0,210)	(0,215)	(0,213)	(0,218)	(0,221)	(0,221)
Alti investimenti tec.	0,902***	0,862***	0,913***	0,933***	0,870***	0,943***
	(0,175)	(0,182)	(0,181)	(0,180)	(0,183)	(0,187)
Basso fatturato all'exp.	0,105	0,0601	0,0355	0,282	0,181	0,181
	(0,181)	(0,190)	(0,186)	(0,203)	(0,215)	(0,209)
Alto fatturato all'exp.	0,241	0,131	0,250	0,300	0,162	0,271
	(0,186)	(0,194)	(0,188)	(0,223)	(0,240)	(0,228)
Fatturato totale	2,293***	2,908***	2,234***	1,437***	1,648***	1,411***
	(0,783)	(0,997)	(0,829)	(0,363)	(0,560)	(0,330)
Controlli	no	no	no	sì	sì	sì
Osservazioni	1.661	1.644	1.641	1.661	1.644	1.641

Note: Coefficienti stimati dall'equazione relativa alla spesa sostenuta per sicurezza cibernetica; standard error robusti in parentesi. *** p<0.01, ** p<0.05, * p<0.1. I controlli includono dummy di settore, area geografica di residenza ("centro nord" e "sud e isole") e di dimensione ("piccola", "media" o "grande").

La variabile $FatturatoExport_i$ misura l'esposizione sui mercati esteri, inclusi quelli in cui la protezione dei dati sensibili è un elemento cruciale dell'organizzazione dell'attività d'impresa, come la Cina o la Russia[15]. La relazione tra investimenti in sicurezza cibernetica e dimensione aziendale può dipendere da numerosi fattori, come il perimetro di esposizione (un'impresa con molti dipendenti

[14] La variabile è definita come la quota di investimenti tecnologici sul totale e prende 5 valori (il valore "non so non rispondo" non viene preso in considerazione): 0=nessun investimento in tecnologie avanzate; 1=tra 0,1 per cento e 5 per cento; 2=tra 5,1 per cento e 20 per cento; 3=tra 20,1 per cento e 40 per cento; 4=oltre 40 per cento.

[15] La variabile prende 4 valori, da "l'azienda non esporta" a "l'azienda realizza più di due terzi del proprio fatturato all'estero". Un insieme di leggi di sicurezza nazionale cinesi, per esempio, impone obblighi di localizzazione e di condivisione anche in assenza di esplicito mandato giudiziario delle informazioni conservate sui sistemi informatici aziendali. Ciò ha spinto numerose imprese a isolare i sistemi informatici relativi alle operazioni in Cina da quelli del resto del mondo, come rilevato dall'indagine sulle imprese europee condotta dalla Camera di Commercio EU in Cina.

può avere più *entry point* per un attaccante), la visibilità, l'appetibilità delle informazioni in proprio possesso. Nell'analisi controlliamo sempre per il fatturato totale. Inoltre, in alcune specificazioni includiamo anche controlli per la dimensione della compagine aziendale, il settore di appartenenza e l'area geografica di residenza della sede amministrativa (ultime tre colonne)[16].

L'occorrenza di un attacco informatico ha un effetto statisticamente significativo sulla spesa solo se non si considerano altre variabili rilevanti, come i controlli per le caratteristiche individuali e la rischiosità dichiarata escludendo così l'ipotesi di un effetto diretto. Come atteso, la percezione che le imprese hanno del rischio che corrono è positivamente correlata con la spesa così come gli investimenti in tecnologie digitali. Il livello di investimenti tecnologici dichiarati dall'azienda risulta sempre significativo ancorché decrescente nella dimensione della quota; nell'interpretazione di questi coefficienti si rimanda alla nota di cautela fatta in precedenza per la possibile fonte di endogeneità. Infine, il fatturato conseguito all'estero non fornisce un contributo significativo. Analizzando la componente panel delle imprese che hanno risposto a tutte le edizioni dell'indagine in cui è stato osservato il fenomeno degli attacchi cybernetici (2016-2022 ad esclusione del 2021; si tratta di circa 500 imprese), risulta che le imprese che hanno subito un attacco nel periodo 2016-2020 hanno sostenuto nel biennio 2021-2022 una spesa per tutelarsi dagli attacchi maggiore di quelle che non ne hanno subiti e la quota di quelle che non hanno speso nulla è la metà rispetto a quelle senza attacchi.

Per trarre informazioni sulla dinamica della spesa, alle imprese è stato chiesto:

Domanda 4

Come è variata negli ultimi 5 anni la spesa per l'acquisto di beni e servizi finalizzata ad incrementare la sicurezza informatica e prevenire incidenti IT della Vostra azienda?

(a) Non è sostanzialmente cresciuta *(b) È cresciuta ma meno che raddoppiata*
(c) È più che raddoppiata

Nel quinquennio 2018-2022, l'indice dei prezzi alla produzione al netto di costruzioni e beni energetici è cresciuto cumulativamente del 19 per cento, più del 12 per cento nel solo 2022. È quindi verosimile che le imprese che hanno dichiarato una spesa costante rispetto a cinque anni prima non stiano beneficiando di un livello di sicurezza superiore, nonostante lo sviluppo tecnologico che ha interessato il mercato dei prodotti per la sicurezza cibernetica. Invece, le imprese che hanno raddoppiato o più la propria spesa potrebbero aver incrementato in maniera significativa la propria copertura verso questo rischio.

[16] La variabile dimensionale è categorica e distingue tra piccole (meno di 50 addetti), medie (50-499 addetti) e grandi imprese (oltre 500 addetti) imprese.

Tav. 8: Variazione spesa sostenuta contro attacchi cibernetici negli ultimi 5 anni
(*quota percentuale di imprese*)

	(1) Non è sostanzialmente cresciuta	(2) È cresciuta, ma meno che raddoppiata	(3) È più che raddoppiata	(4) Numero risposte
Area geografica				
Centro Nord	45,6	41,1	13,3	1.100
Sud e Isole	67,4	25,7	6,9	625
Numero di addetti				
20 – 49	56,4	33,2	10,4	559
50 e oltre	36,6	48,1	15,4	1.166
Totale industria in s.s e servizi	**49,7**	**38,2**	**12,1**	**1.725**

Note: Statistiche ponderate per i pesi di riporto al numero delle imprese dell'universo.

In Tav. 8 sono riportate statistiche descrittive relative alla domanda sulla dinamica della spesa nell'ultimo quinquennio. Per circa metà delle imprese la spesa è rimasta sostanzialmente costante, mentre solo un ottavo ha più che raddoppiato le risorse dedicate alla sicurezza cibernetica.

Tav. 9: Analisi di regressione non lineare (ordered logit): dinamica della spesa in sicurezza cibernetica

	(1)	(2)	(3)	(4)	(5)	(6)
Basso rischio dichiarato	2,168***					1,761***
	(0,459)					(0,497)
Alto rischio dichiarato	3,848***					3,174***
	(0,527)					(0,567)
Attacco		1,321***				0,701**
		(0,281)				(0,289)
Funzione aziendale			1,410***			1,326***
			(0,297)			(0,291)
Funzione interna				0,533		
				(0,392)		
Funzione ibrida				-0,122		
				(0,375)		
Bassi investimenti tecnologici					0,631*	0,303
					(0,342)	(0,339)
Alti investimenti tecnologici					0,961***	0,702**
					(0,303)	(0,318)
Spesa(2016) < 10.000€	0,552	0,647*	0,594	0,289	0,681*	0,493
	(0,347)	(0,355)	(0,362)	(0,417)	(0,369)	(0,366)
Spesa(2016) < 50.000€	0,805**	0,814**	1,042***	0,625	1,079***	0,610
	(0,384)	(0,381)	(0,384)	(0,451)	(0,387)	(0,388)
Spesa(2016) < 200.000€	1,021**	1,262***	1,365***	1,013**	1,653***	0,568
	(0,450)	(0,443)	(0,406)	(0,457)	(0,434)	(0,428)
Spesa(2016) > 200.000€	-0,351	0,273	0,404	-0,514	0,493	0,0824
	(0,823)	-1031	-1369	-1275	-1056	-1000
Fatturato	0,105	0,121	0,115	0,151	0,121	0,0442
	(0,121)	(0,187)	(0,170)	(0,145)	(0,177)	(0,0966)
Controlli	sì	sì	sì	sì	sì	sì
Osservazioni	822	821	820	602	800	794

Note: Coefficienti stimati dall'equazione relativa alla dinamica della spesa sostenuta per sicurezza cibernetica; standard error robusti in parentesi. *** p<0.01, ** p<0.05, * p<0.1. I controlli includono dummy di settore, area geografica di residenza ("centro nord" e "sud e isole") e di dimensione ("piccola", "media" o "grande").

In Tav. 9 sono riportate le stime dei coefficienti di regressione di un modello *ordered logit* che relaziona la dinamica della spesa per sicurezza cibernetica nell'ultimo quinquennio con una serie di variabili (contemporanee e passate) e misure di sensibilità al problema, come la percezione dichiarata del rischio, l'essere stato oggetto di un attacco o la presenza di una funzione dedicata[17]. La natura della funzione dedicata alla sicurezza (se interna, esterna o ibrida) non risulta una variabile statisticamente significativa; al contrario, la probabilità di aumentare la propria spesa cresce con la quota di investimenti tecnologici sul totale.

Il livello della spesa nel 2016 risulta positivamente e significativamente correlato con la dinamica della stessa nel quinquennio 2018-22 per quelle imprese che spendevano importi compresi tra 10 mila e 200 mila euro. Le imprese con un livello di spesa inferiore a 10 mila euro nel 2016, probabilmente perché scarsamente motivate a proteggersi verso il rischio cibernetico, dimostrerebbero una persistente bassa considerazione del problema. Al contrario, imprese con un livello di spesa già sostenuto nel 2016 (superiore a 200 mila euro) hanno verosimilmente ritenuto non necessario aumentare ulteriormente il proprio impegno.

Infine, alle imprese è stato chiesto di quale strumento si sono dotate per far fronte al rischio di attacchi cibernetici:

Domanda 5

Avete una funzione aziendale (anche eventualmente in outsourcing) dedicata al governo e alla gestione della cyber-sicurezza e della continuità operativa?

(a) No	*(b) Sì, completamente interna all'azienda*[18]
(c) Sì, in parte interna in parte in outsourcing	*(d) Sì, interamente in outsourcing*

In linea di principio, una funzione esterna o parzialmente interna al perimetro aziendale rappresenta una fonte di vulnerabilità per l'azienda in ragione del fatto che questa dovrà condividere con soggetti esterni un certo numero di informazioni sensibili. Tuttavia, per aziende con minori capacità finanziarie livelli di protezione sofisticati potrebbero essere accessibili solo esternalizzando totalmente o parzialmente tale funzione. Una nota di cautela nel leggere le risposte a questa domanda va posta sul fatto che alle imprese si chiede di riferire non solo in merito alla gestione della sicurezza cibernetica ma anche alla continuità operativa, funzioni che possono richiedere infrastrutture differenti e, di conseguenza, favorire il ricorso a una gestione ibrida.

[17] La domanda posta alle imprese (come si vedrà più avanti) non consente di individuare quando l'impresa si è dotata della funzione, rendendo difficile stabilire se l'incremento della spesa sia stato dovuto alla creazione di tale funzione oppure sia generato dalla funzione stessa.

[18] Ancorché si possa avvalere di fornitori esterni, la funzione dedicata è considerata interna se questa si assume la responsabilità ultima di qualsiasi incidente di natura cibernetica dovesse interessare l'azienda.

Tav. 10: Funzione aziendale dedicata alla cybersicurezza e alla continuità operativa
(*quota percentuale di imprese*)

		Sì			
	(1)	(2)	(3)	(4)	(5)
	No	Completamente interna	Ibrida	Completamente in outsourcing	Numero risposte
Area geografica					
Centro Nord	4,7	52,3	42,4	5,4	1.116
Sud e Isole	5,6	70,1	23,4	6,5	633
Numero di addetti					
20 - 49	4,3	77,3	18,9	3,8	562
50 e oltre	5,8	47,3	46,8	6,0	1.187
Totale industria in s.s e servizi	**4,8**	**54,0**	**40,5**	**5,5**	**1.749**

Note: statistiche ponderate per i pesi di riporto al numero delle imprese dell'universo.

In Tav. 10 sono riportate statistiche descrittive relative alla scelta di dotarsi o meno di una funzione aziendale dedicata. Nel complesso, più di un terzo delle imprese non è dotata di una funzione aziendale dedicata alla sicurezza cibernetica e alla continuità operativa. Tra quelle che hanno risposto affermativamente, la maggior parte delle aziende usufruiscono di una funzione interna o ibrida, mentre la quota di quelle che ne hanno una in completo outsourcing è nettamente inferiore.

Sulla base di un modello logit bivariato, si analizza prima la scelta di dotarsi di una funzione aziendale dedicata alla sicurezza cibernetica e, in seguito, quella di adottare una soluzione esternalizzata (scenario di base), una ibrida o una completamente interna. I tre modelli si basano sullo stesso set di regressori che, oltre a una serie di *dummy* per settore di appartenenza, regione di residenza e numero di addetti, include: l'essere stati oggetto di un attacco, averne o meno subito danni patrimoniali, livello di rischio dichiarato, quota di investimenti tecnologici sul totale.

Le stime dei coefficienti di regressione sono riportate in Tav. 11. La percezione del rischio e l'essere stato oggetto o meno di un attacco sono correlate significativamente con la decisione di dotarsi di una funzione dedicata, così come la dimensione della compagine e l'area geografica (imprese del centro e del sud sono più riluttanti). I risultati relativi alla scelta del tipo di funzione sembrano più difficili da interpretare: la probabilità di rimanere nello scenario di base (ovvero l'adozione di una funzione interamente esternalizzata) sembra crescere con il livello di rischio dichiarato, mentre la dimensione dell'impresa è positivamente correlata con la scelta di avere all'interno dell'azienda almeno parte della funzione dedicata.

Tav. 11: Analisi di regressione non lineare (ordered logit): rischio cibernetico dichiarato

		Tipo di funzione	
	(1)	(2)	(3)
	Sì/No	Ibrida	Interna
Attacco	0,784***	0,969***	0,655***
	(0,174)	(0,223)	(0,227)
Basso rischio dichiarato	1,257***	-0,836**	-0,693**
	(0,191)	(0,403)	(0,350)
Alto rischio dichiatato	1,875***	-0,330	-0,770*
	(0,234)	(0,437)	(0,397)
Bassi investimenti tec.	0,0825	1,031***	0,131
	(0,159)	(0,218)	(0,221)
Alti investimenti tec.	0,249*	0,587***	0,479**
	(0,140)	(0,200)	(0,187)
Danni patrimoniali	-0,207	-1,095***	-1,174***
	(0,306)	(0,364)	(0,377)
Nord-est	-0,142	0,214	-0,274
	(0,198)	(0,200)	(0,209)
Centro	-0,486***	-0,870***	-0,0322
	(0,181)	(0,250)	(0,220)
Sud e isole	-0,648***	-0,547**	0,352
	(0,166)	(0,269)	(0,235)
50-200 addetti	0,489***	0,185	0,00506
	(0,131)	(0,180)	(0,176)
Più di 200 addetti	0,738***	1,032***	1,117***
	(0,169)	(0,394)	(0,390)
Costante	-0,698	-0,856	0,895**
	(0,444)	(0,619)	(0,429)
Osservazioni	1.430	1.465	1.430

Note: Stima dei coefficienti del modello di scelta sulla funzione aziendale dedicata. Note: Standard errors robusti in parentesi. *** p<0.01, ** p<0.05, * p<0.1. Tutte le equazioni includono variabili dummy di settore.

4. Conclusioni

La consapevolezza dei rischi cibernetici appare largamente diffusa tra le imprese, sebbene in misura diversa tra classi dimensionali e aree geografiche. Solo una piccola quota si ritiene al riparo dagli attacchi cyber, tra queste soprattutto le imprese piccole e residenti nel sud dell'Italia. Il settore di appartenenza non sembra rilevante per spiegare differenze nei livelli di consapevolezza. Nonostante le rilevazioni INVIND condotte tra il 2016 e il 2020 non siano sovrapponibili con quella sul 2022, confrontando i risultati sembrerebbe che il numero di attacchi cibernetici sia su un trend decrescente. La consapevolezza del rischio cibernetico è maggiore per le imprese che sono state oggetto di un attacco da parte di agenti malevoli; pur nella difficoltà di comprenderne a pieno la direzione causale, la dotazione di un livello più elevato di tecnologia è associata a una maggiore comprensione del pericolo cibernetico.

La consapevolezza dichiarata dalle imprese stenta tuttavia a tradursi nell'adozione di azioni concrete: anche se il trend degli attacchi risulta in diminuzione negli ultimi cinque anni, la natura mutevole del

fenomeno richiede aggiornamenti costanti dei sistemi di protezione che, vista la loro complessità, hanno costi sempre maggiori. L'indagine INVIND sul 2022 mostra che la spesa per l'acquisizione di presidi contro la minaccia cyber continua a essere piuttosto contenuta. Più di un terzo delle aziende continua a non avere una funzione aziendale dedicata, né interna né esterna. Anche se metà delle imprese dichiarano di aver aumentato la spesa in sicurezza cibernetica nell'ultimo quinquennio, è plausibile ipotizzare che ciò sia dovuto più alla crescita dei costi per l'acquisizione di attrezzature hardware e software che a un incremento della domanda per questo tipo di servizi. I soggetti che sembrano avere maggiore difficoltà ad adottare misure per ridurre il rischio cibernetico, anche a seguito di attacchi subiti, sono quelli con una minore percezione del rischio, ovvero le aziende di minore dimensioni e, soprattutto, residenti nel meridione.

Riferimenti bibliografici

Banca d'Italia (2023), "*Indagine sulle imprese industriali e dei servizi nell'anno 2022*", Collana Statistiche, 30 Giugno 2023.

Biancotti, C. (2017), "*Cyber attacks: preliminary evidence from the Bank of Italy's business surveys*", Banca d'Italia, Questioni di Economia e Finanza, No. 373, Febbraio.

Biancotti, C. (2017), "*The price of cyber (in)security: evidence from the Italian private sector*", Banca d'Italia, Questioni di Economia e Finanza, No. 407, Novembre.

European Chamber of Commerce in China (2023), "*European business in China - Business confidence survey 2023*", Maggio 2023.

Sistema di informazione per la sicurezza della Repubblica (2023), "*Relazione sulla politica dell'informazione per la sicurezza relativa al 2022*", Relazione al Parlamento 2022, 28 Febbraio 2023.