CYBERSECURITY

LA SICUREZZA IT PER LE PMI

PID cyber Check

Consiglio Nazionale delle Ricerche (CNR)

Cybersecurityosservatorio.it

Consiglio Nazionale
delle Ricerche

SOMMARIO

- Collaborazione tra PID e Osservatorio sulla cybersecurity del CNR
- La cyber security come crescente tema sociale, economico e non solo tecnologico
- Evoluzione delle minaccie anche e soprattuto per le PMI
- Lo strumento PID Cyber Check come strumento per comprendere la propria postura di sicurezza

Consiglio Nazionale delle Ricerche

IL PIÙ GRANDE ENTE PUBBLICO DI RICERCA IN ITALIA

QUASI 100 ISTITUTI DI RICERCA PRESENTI IN TUTTA ITALIA

TUTTE LE AREE DELLE SCIENZA COPERTE, INCLUSA OVVIAMENTE LA CYBER SECURITY

CIRCA 10.000 TRA RICERCATORI, TECNICI E PERSONALE AMMINISTRATIVO

CYBER SECURITY OSSERVATORIO

Consiglio Nazionale delle Ricerche

Osservatorio sulla cyber security del CNR

- Una piattaforma web per raccogliere e fornire informazioni i servizi per la cyber security
  - Serve per accrescere la **consapevolezza** di cittadini e (piccole/medie) industrie
  - Con la base ed il supporto tecnologico di progetti di ricerca Regionali (Toscana), Nazionali ed Europei come C3ISP e SPARTA

“Cybersecurity is no longer a technological ‘option’, but a societal need”

CYBER SECURITY OSSERVATORIO

Consiglio Nazionale delle Ricerche

PERCHÉ IL PROBLEMA DELLA SICUREZZA

Oggi la rete informatica è entrata nelle **case** di molti, è utilizzata dalle **società**, dagli **Enti pubblici** e **privati**, anche come mezzo per transazioni commerciali.

Molte infrastrutture critiche come il sistema energetico dipendono dalla sicurezza

CYBER SECURITY OSSERVATORIO

Consiglio Nazionale delle Ricerche

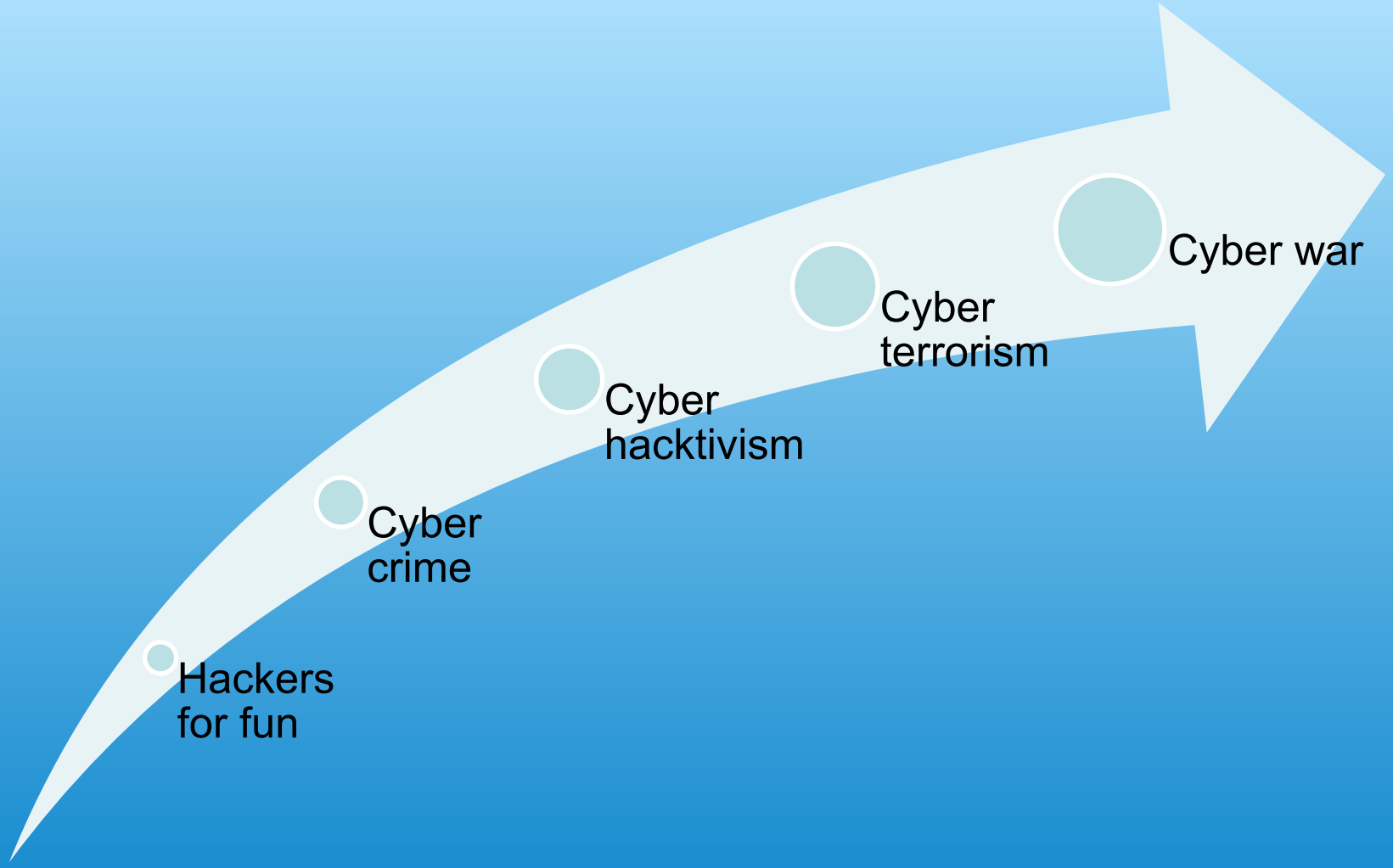
VULNERABILITÀ, ATTACCHI E MINACCE

VULNERABILITÀ (VULNERABILITY):
DEBOLEZZA DI UN SISTEMA DI SICUREZZA CHE PUÒ ESSERE UTILIZZATA PER CAUSARE DANNI

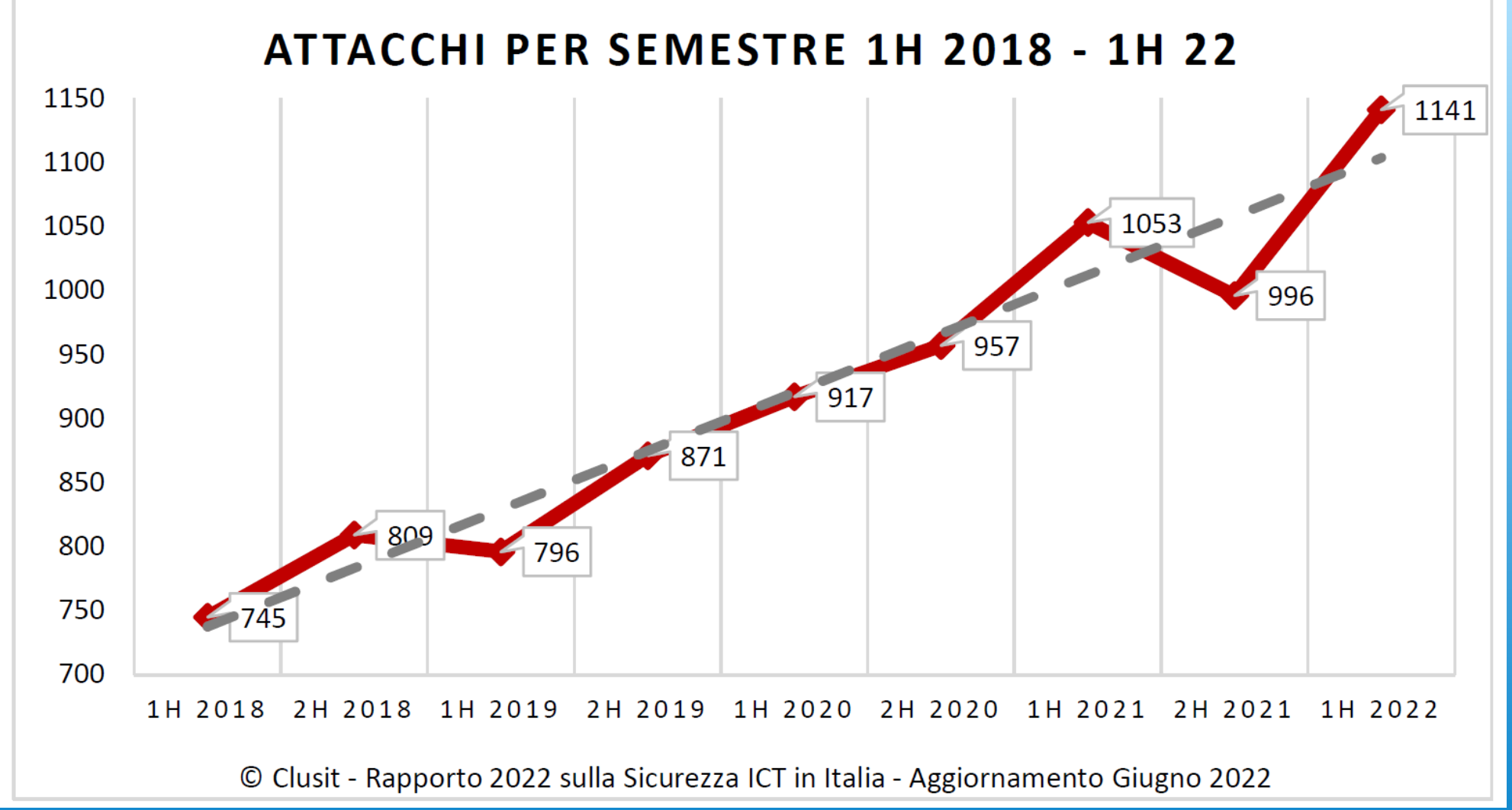
ATTACCO (ATTACK): SFRUTTAMENTO DI UNA VULNERABILITÀ DI UN SISTEMA

MINACCIA (THREAT):
ENTITÀ/CIRCOSTANZA CHE PUÒ CAUSARE DANNI (ATTACCO, DISASTRO NATURALE, …)

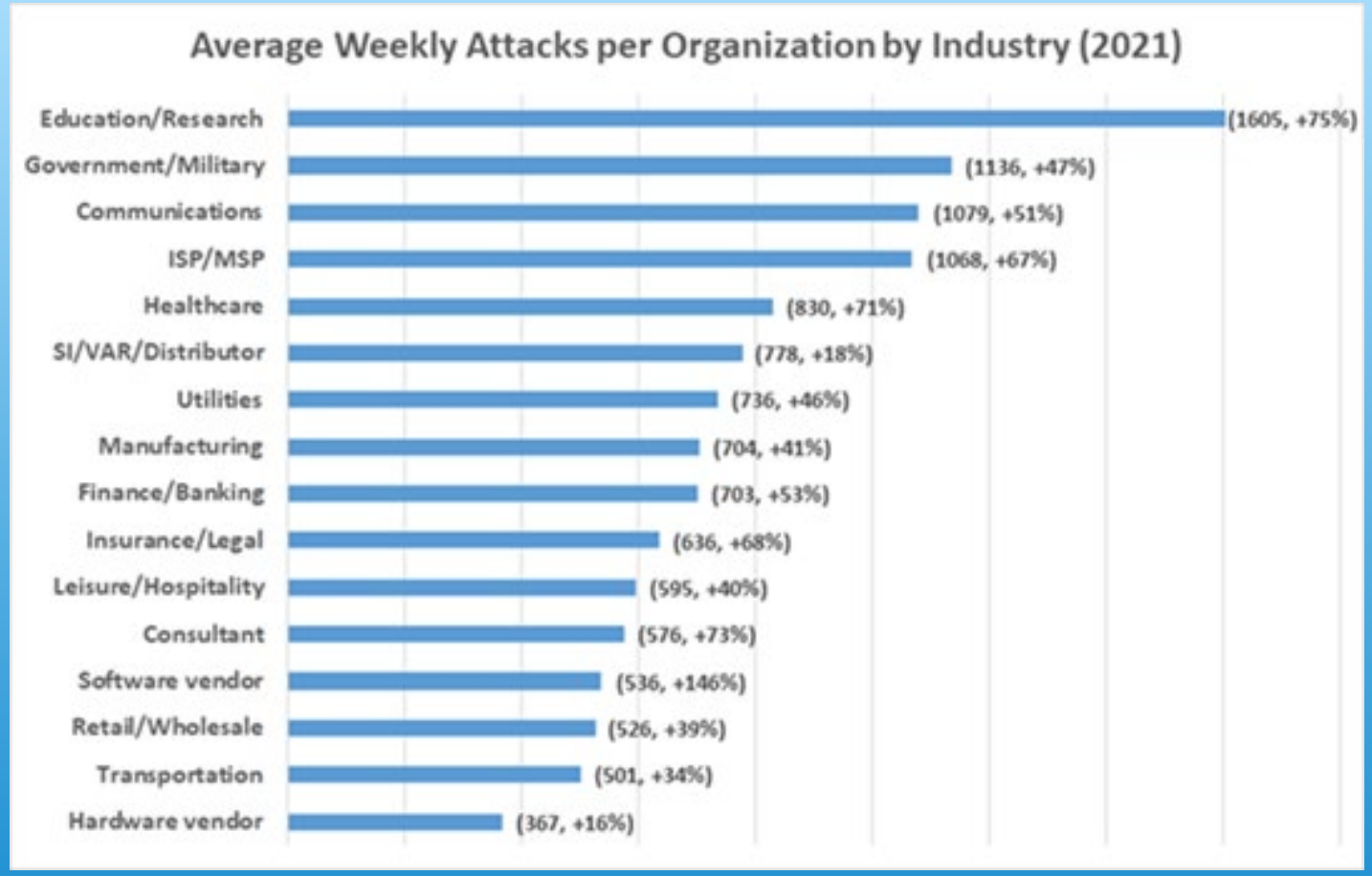
Evoluzione delle minacce



Crescita continua degli attacchi gravi



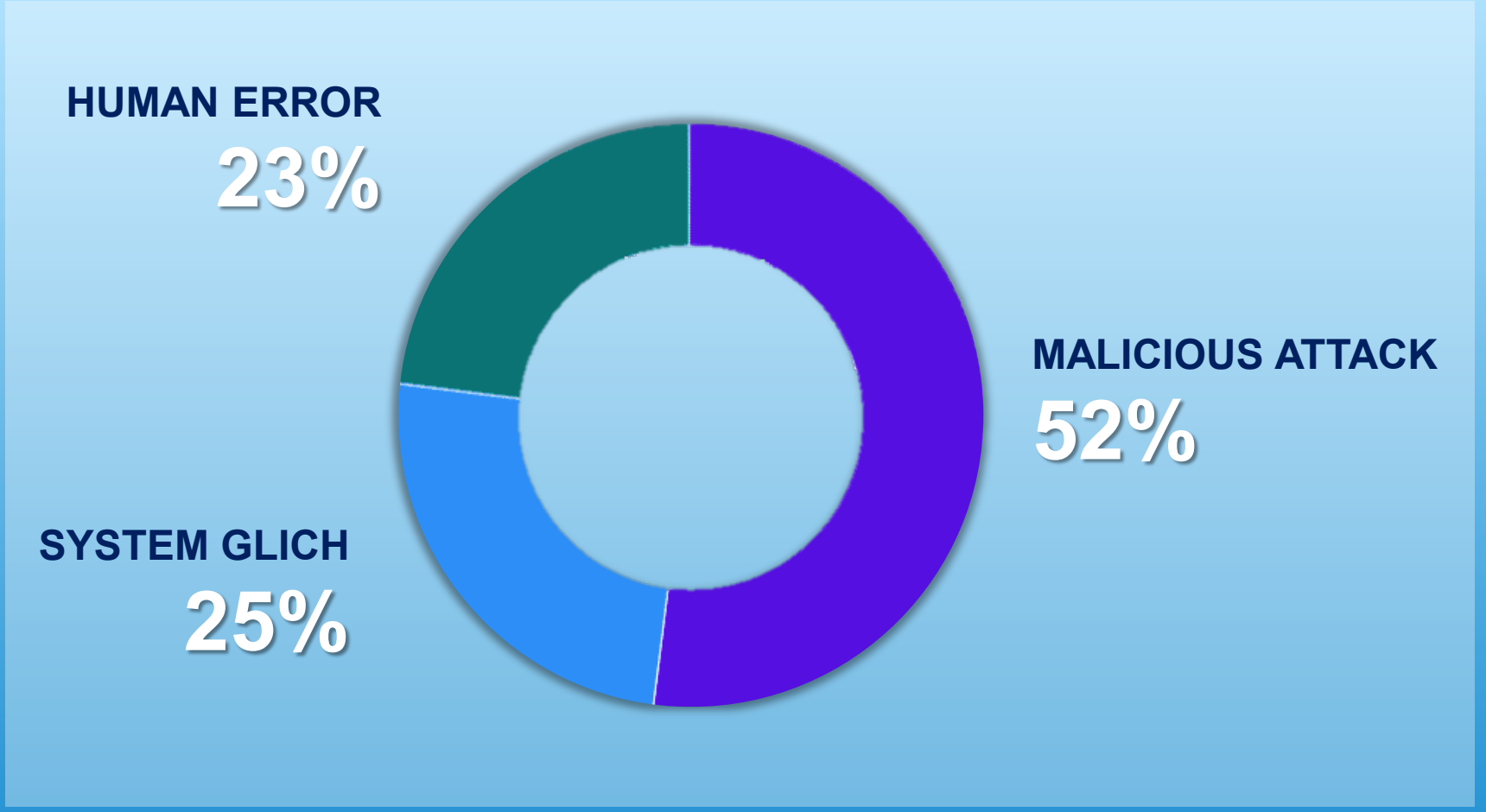
Sectors



https://channels.theinnovationgroup.it/cybersecurity/grande-crescita-attacchi-cyber-2021/

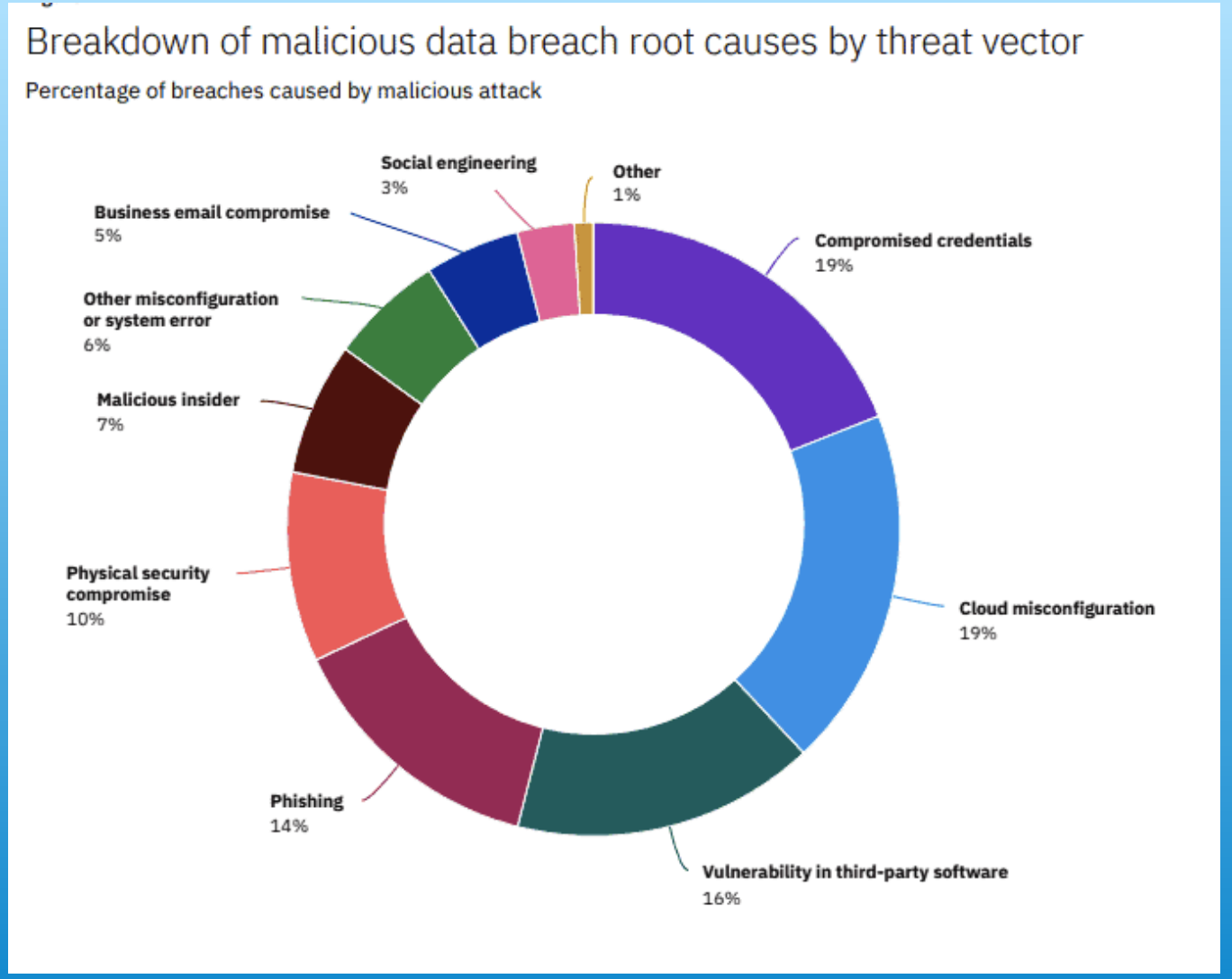
DATA BREACHES/LEAKS

DATA BREACH ROOT COUSE BREAKDOWN IN THREE CATEGORIES



https://www.metacompliance.com/blog/calculating-the-heavy-cost-of-data-breaches-in-2021/

Vettori di attacco per data breaches

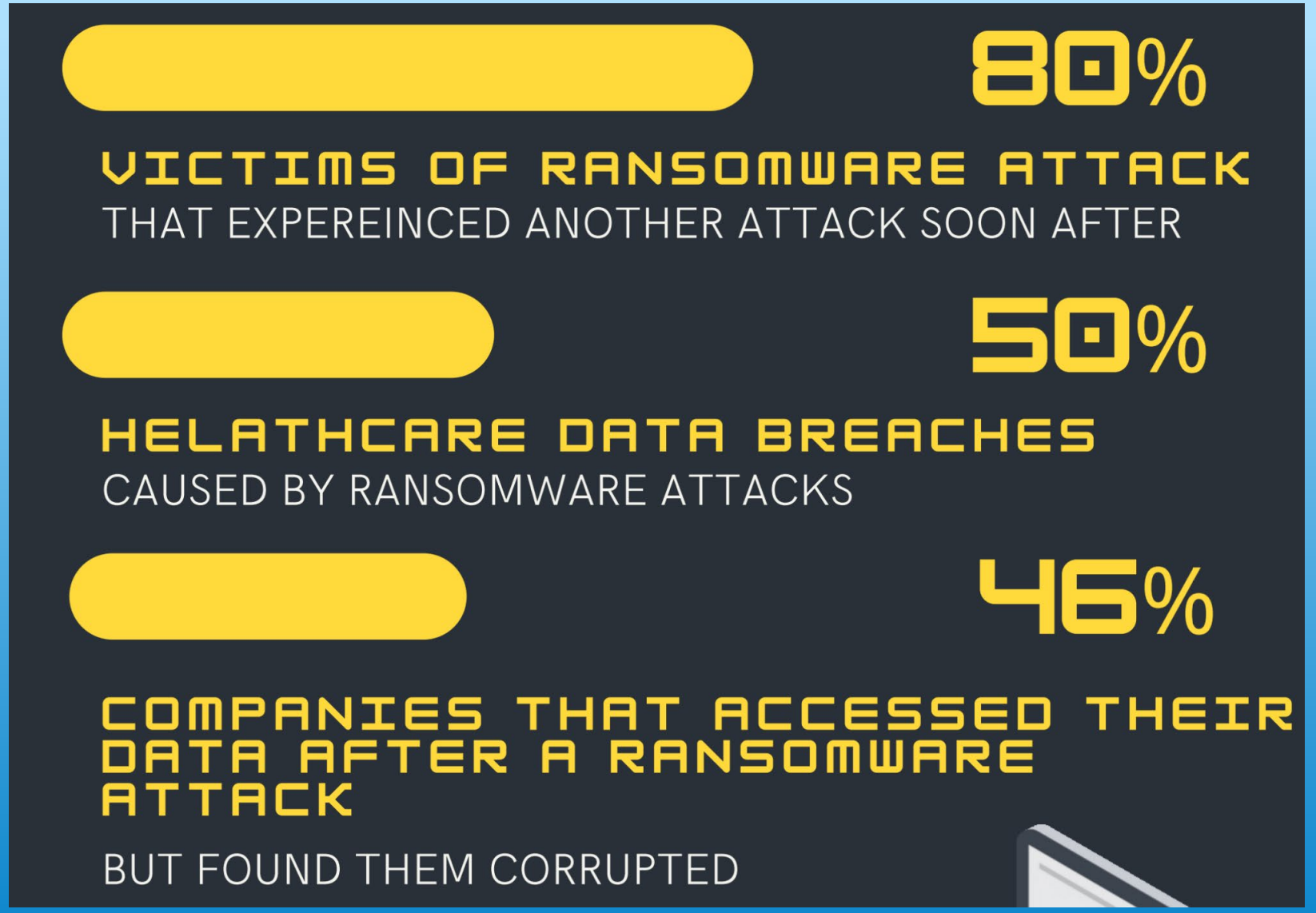


https://www.metacompliance.com/blog/calculating-the-heavy-cost-of-data-breaches-in-2021/

Tempo medio per rimediare ad un attacco

- 60 giorni nel 2022
- 40 giorni nel 2015

Alcuni dati sul ransomware



Vulnerabilità registrate

- Le vulnerabilità note vengono catalogate dal MITRE
  - https://cve.mitre.org/
- Circa 170.000 (accessibili anche dal cybersecurity osservatorio.it)
- Le vulnerabilità hanno anche uno score che ne determina la rilevanza

Vulnerabilities

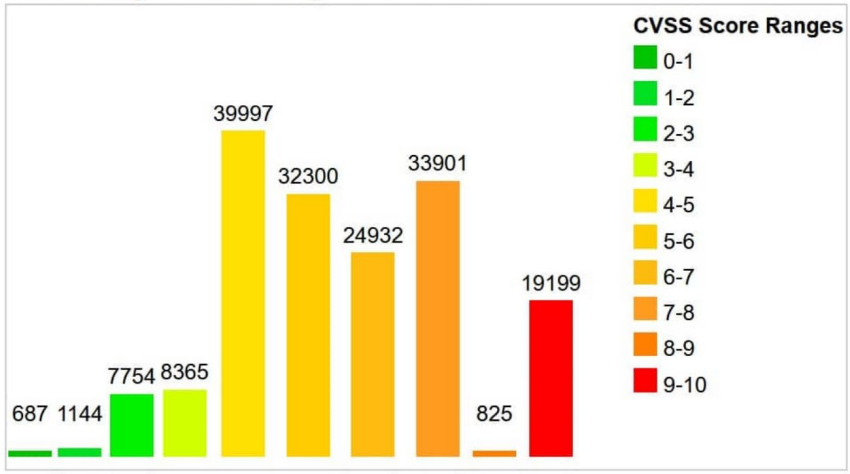
Current CVSS Score Distribution For All Vulnerabilities

Distribution of all vulnerabilities by CVSS Scores

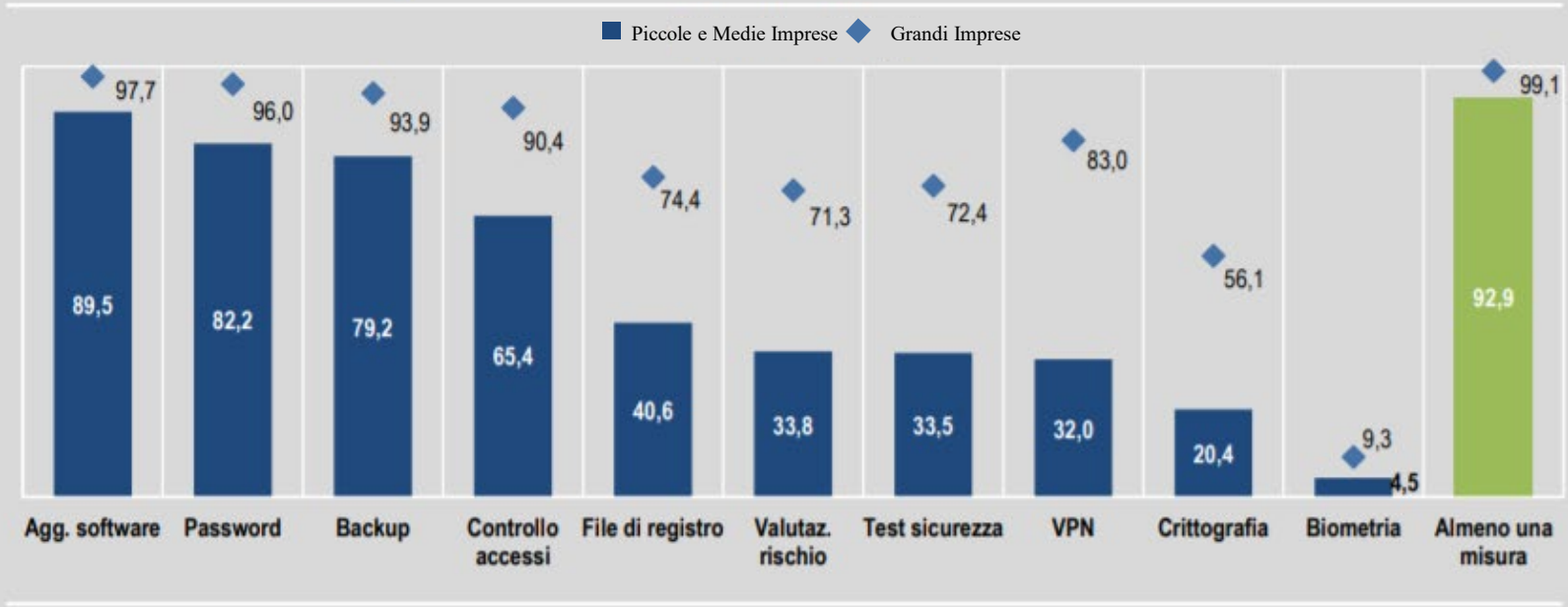
CVSS Score	Number Of Vulnerabilities	Percentage
0-1	687	0.40
1-2	1144	0.70
2-3	7754	4.60
3-4	8365	4.90
4-5	39997	23.70
5-6	32300	19.10
6-7	24932	14.70
7-8	33901	20.00
8-9	825	0.50
9-10	19199	11.40
Total	169104	

Weighted Average CVSS Score: **6.5**

Vulnerability Distribution By CVSS Scores



Misure di sicurezza informatica per tipo di misura e classe di addetti



https://channels.theinnovationgroup.it/cybersecurity/istat-misure-minime-cybersecurity-pmi/

Misure Minime Di Cybersecurity

Solo 68% delle PMI adotta almeno 3 misure di sicurezza:

- utilizzo di password complesse per autenticazione;
- aggiornamento del software;
- backup dei dati.

	Imprese che utilizzano tre misure minime [a] di sicurezza ICT
10-49	68,0
50-99	85,1
100-249	87,1
250 e più	90,8

(a) Imprese che utilizzano le tre seguenti misure di sicurezza: password complessa, aggiornamento software, backup.

Fonte: Rilevazione sulle tecnologie dell'informazione e della comunicazione nelle imprese, Anno 2019

https://channels.theinnovationgroup.it/cybersecurity/istat-misure-minime-cybersecurity-pmi/

Valutazione del rischio ICT

	Imprese che effettuano una valutazione del rischio ICT
10-49	30,7
50-99	51,8
100-249	61,4
250 e più	71,3

Fonte: Rilevazione sulle tecnologie dell'informazione e della comunicazione nelle imprese, Anno 2019

	Imprese che effettuano test di sicurezza ICT
10-49	30,6
50-99	49,1
100-249	58,4
250 e più	72,4

Fonte: Rilevazione sulle tecnologie dell'informazione e della comunicazione nelle imprese, Anno 2019

https://channels.theinnovationgroup.it/cybersecurity/istat-misure-minime-cybersecurity-pmi/

Prontezza informatica di PMI

- Realta
  - L'85% delle violazioni dei dati colpisce le piccole imprese
  - Il 60% delle piccole imprese colpite da un attacco informatico si è spento entro sei mesi
  - le piccole e medie imprese stanno perdendo $ 120.000 per incidente informatico

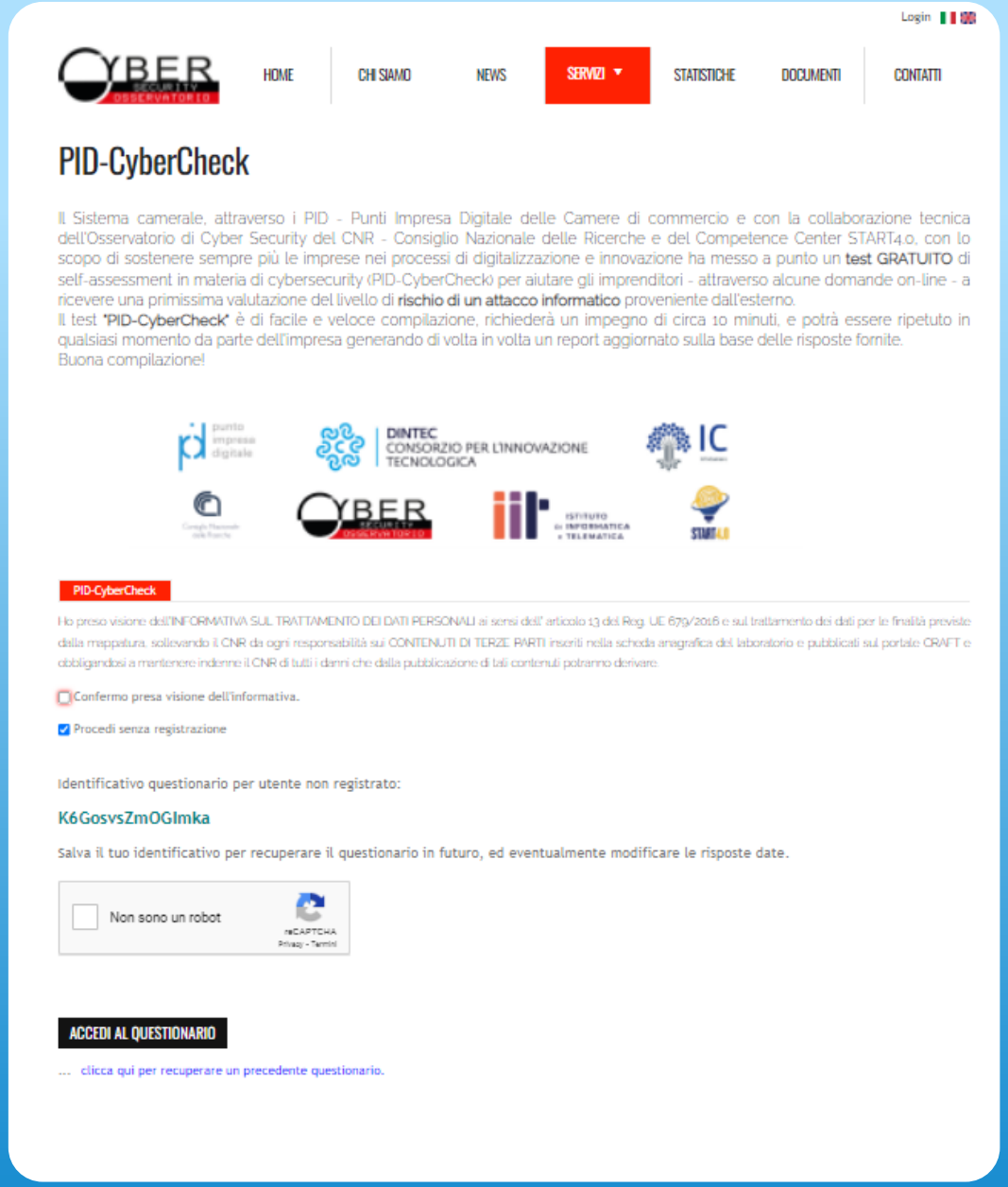
- risposta agli incidenti
  - Solo Il 54% non hanno un piano in atto per affrontare un attacco informatico
  - Altri Il 20% dicono che reagirano quando succede qualcosa

https://www.insurancebee.com/blog/smb-owners-unprepared-for-cybercrime

LO STRUMENTO DI ANALISI DEI RISCHI

LO SCOPO

LO SCOPO PRINCIPALE DEL NOSTRO STRUMENTO È QUELLO DI OFFRIRE UN MODO SEMPLICE E VELOCE PER EFFETTUARE UN **SELF-ASSESSMENT DEI CYBER RISCHI** E **OTTIMIZZARE** GLI **INVESTIMENTI IN SICUREZZA CYBER**.



CYBER SECURITY OSSERVATORIO

Consiglio Nazionale delle Ricerche

PID CYBER CHECK - REPORT

CHECKUP Sicurezza IT — PID Cyber Check

punto impresa digitale | DINTEC CONSORZIO PER L'INNOVAZIONE TECNOLOGICA

CHECKUP Sicurezza IT — PID Cyber Check

REPORT PER L'AZIENDA

ACME SPA

REDATTO IN BASE AI DATI FORNITI IL:

19 maggio 2022

CODICE PER RECUPERARE IL QUESTIONARIO:

twkjj12093sdfj

Se il questionario è stato compilato senza registrazione, la stringa qua sopra può essere utilizzata per recuperare le risposte ed eventualmente aggiornarle/modificarle

punto impresa digitale | DINTEC CONSORZIO PER L'INNOVAZIONE TECNOLOGICA

FINALITÀ DEL REPORT

Il presente report restituisce una valutazione in merito al livello di rischio cibernetico stimato per l'impresa ed elaborato sulla base delle riposte fornite al "**PID-CyberCheck**", il test di autovalutazione online dei PID – Punti Impresa Digitale delle Camere di commercio realizzato con la collaborazione tecnica dell'Osservatorio di Cyber Security del CNR – Consiglio Nazionale delle Ricerche e del Competence Center START4.0.

Il test "PID-CyberCheck" potrà essere ripetuto in qualsiasi momento da parte dell'impresa generando di volta in volta un report aggiornato sulla base delle risposte fornite.

CONTENUTI DEL REPORT

Contenuti del Report

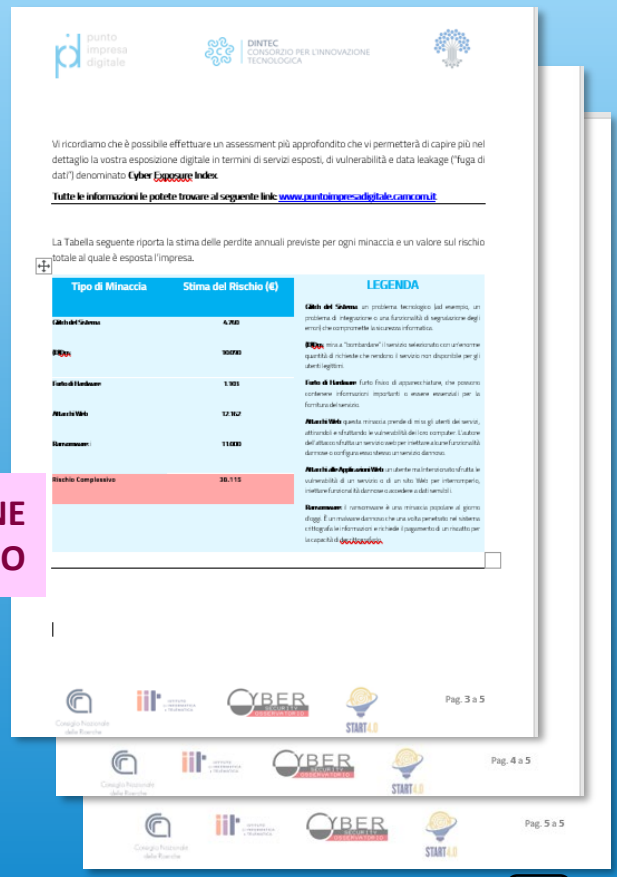
Livello del rischio: 17/100

Di seguito è riportata una breve descrizione dei quadranti di rischio inseriti all'interno della precedente figura che tengono conto delle risposte fornite al "PID-CyberCheck":

RISCHIO BASSO	Un basso livello di rischio vuol dire che l'impresa ha intrapreso la strada corretta in tema di cybersecurity. Tale risultato non deve indurre l'impresa a ritenere di non aver bisogno di un esame approfondito che è fortemente consigliato.
RISCHIO MEDIO	Un medio livello di rischio indica che l'impresa ha ancora ampi margini di miglioramento in tema di cybersecurity. Un esame più approfondito dei sistemi aziendali è necessario per definire le politiche e gli interventi in materia di cyber-security da mettere in atto.
RISCHIO ALTO	Un alto livello di rischio indica che l'impresa ha diverse criticità in tema di cyber-security. Pertanto è fondamentale effettuare ulteriori approfondimenti, sottoponendo l'impresa a sistemi più approfonditi di analisi, e attuare interventi per ridurre il rischio cibernetico.

LIVELLO DI RISCHIO

QUANTIFICAZIONE DEL RISCHIO



punto impresa digitale | DINTEC CONSORZIO PER L'INNOVAZIONE TECNOLOGICA

Vi ricordiamo che è possibile effettuare un assessment più approfondito che vi permetterà di capire più nel dettaglio la vostra esposizione digitale in termini di servizi esposti, di vulnerabilità e data leakage ("fuga di dati") denominato **Cyber Exposure Index**.

Tutte le informazioni le potete trovare al seguente link: www.puntoimpresadigitale.camcom.it

La Tabella seguente riporta la stima delle perdite annuali previste per ogni minaccia e un valore sul rischio totale al quale è esposta l'impresa.

Tipo di Minaccia	Stima del Rischio (€)
Guasto del Sistema	4.700
DDos	10000
Furto di Hardware	1.101
Attacchi Web	12.167
Ransomware	11000
Rischio Complessivo	38.115

LEGENDA

Guasto del Sistema: un problema tecnologico (ad esempio, un problema di integrazione o una funzionalità di segnalazione degli errori) che compromette la sicurezza informatica.

DDos: senza "bombardare" il servizio selezionato con un'enorme quantità di richieste che rendono il servizio non disponibile per gli utenti legittimi.

Furto di Hardware: furto fisico di apparecchiature, che possono contenere informazioni importanti o essere essenziali per la fornitura del servizio.

Attacchi Web: questa minaccia prende di mira gli utenti del servizi, attraverso lo sfruttando le vulnerabilità dei loro computer. L'autore dell'attacco sfrutta un servizio web per inviare alcune funzionalità dannose o configura esso stesso un servizio dannoso.

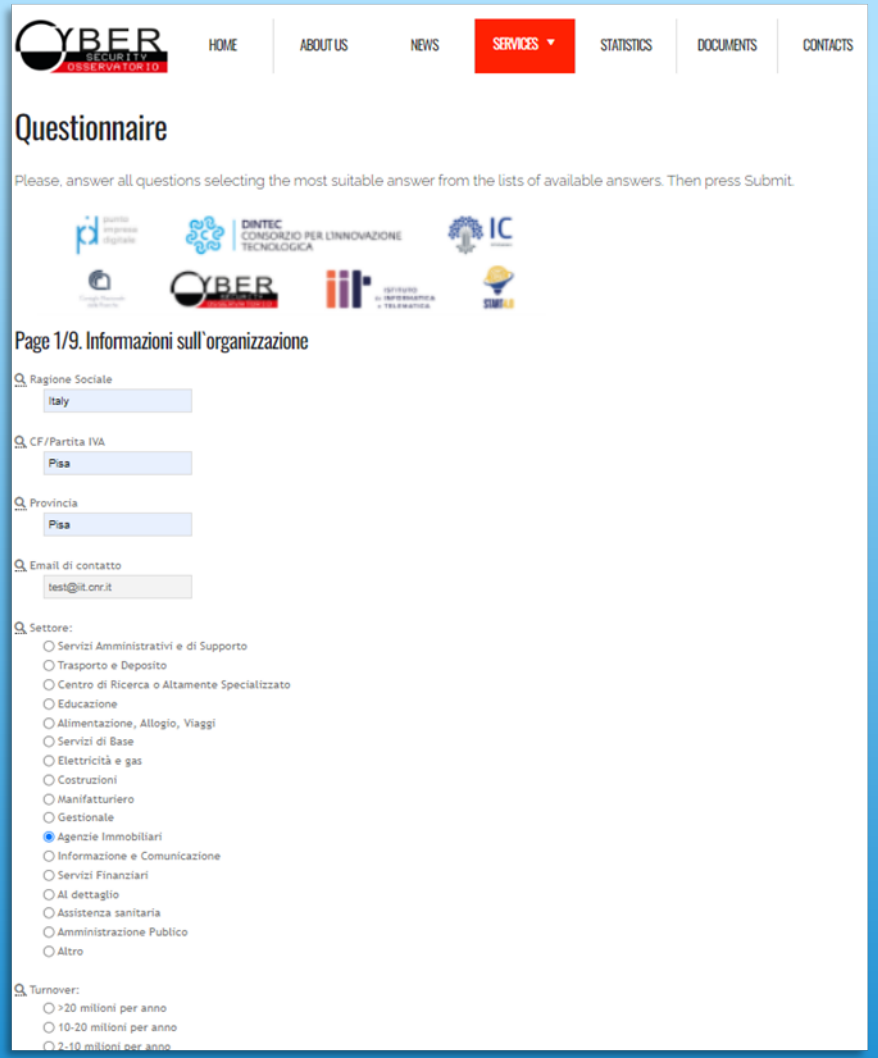
Attacchi alle Applicazioni Web: un utente malintenzionato sfrutta le vulnerabilità di un servizio o di un sito Web per intercettare, inviare funzioni fraudolente o accedere a dati sensibili.

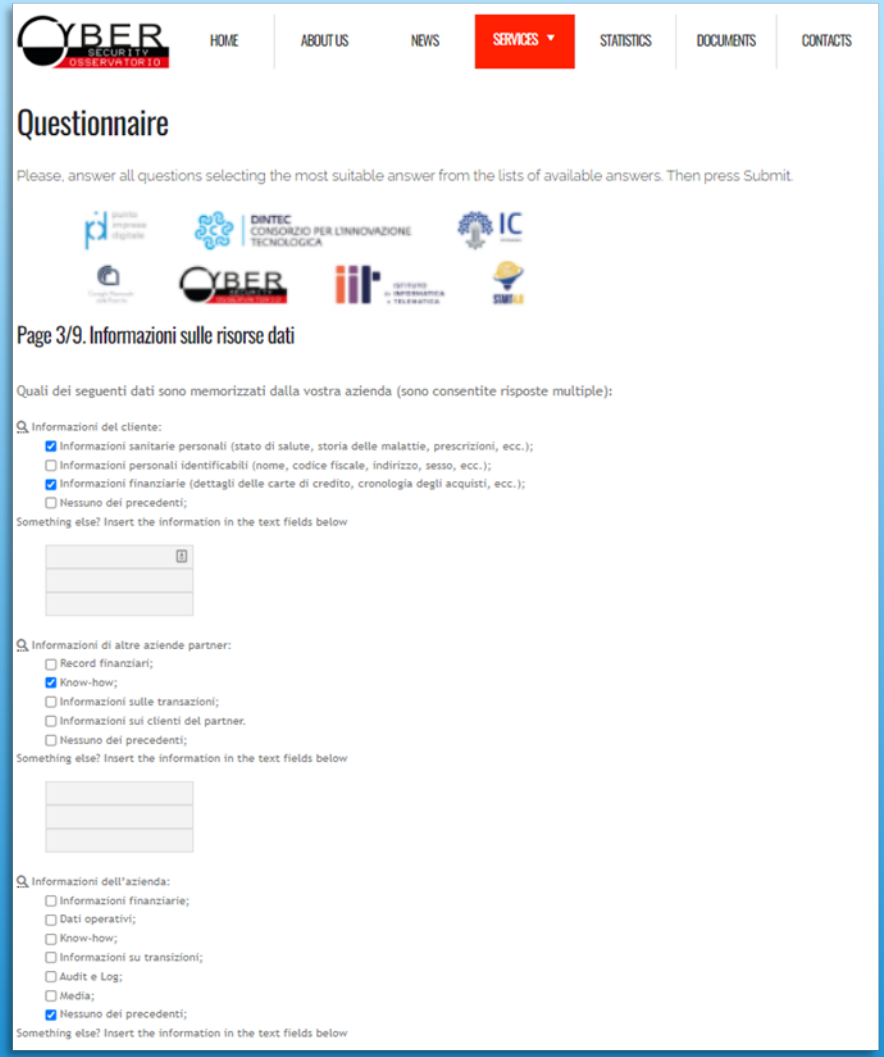
Ransomware: il ransomware è una minaccia presente al giorno d'oggi. È un malware dannoso che una volta penetrato nel sistema crittografa le informazioni e richiede il pagamento di un riscatto per la possibilità di [illegible]

CYBER SECURITY OSSERVATORIO

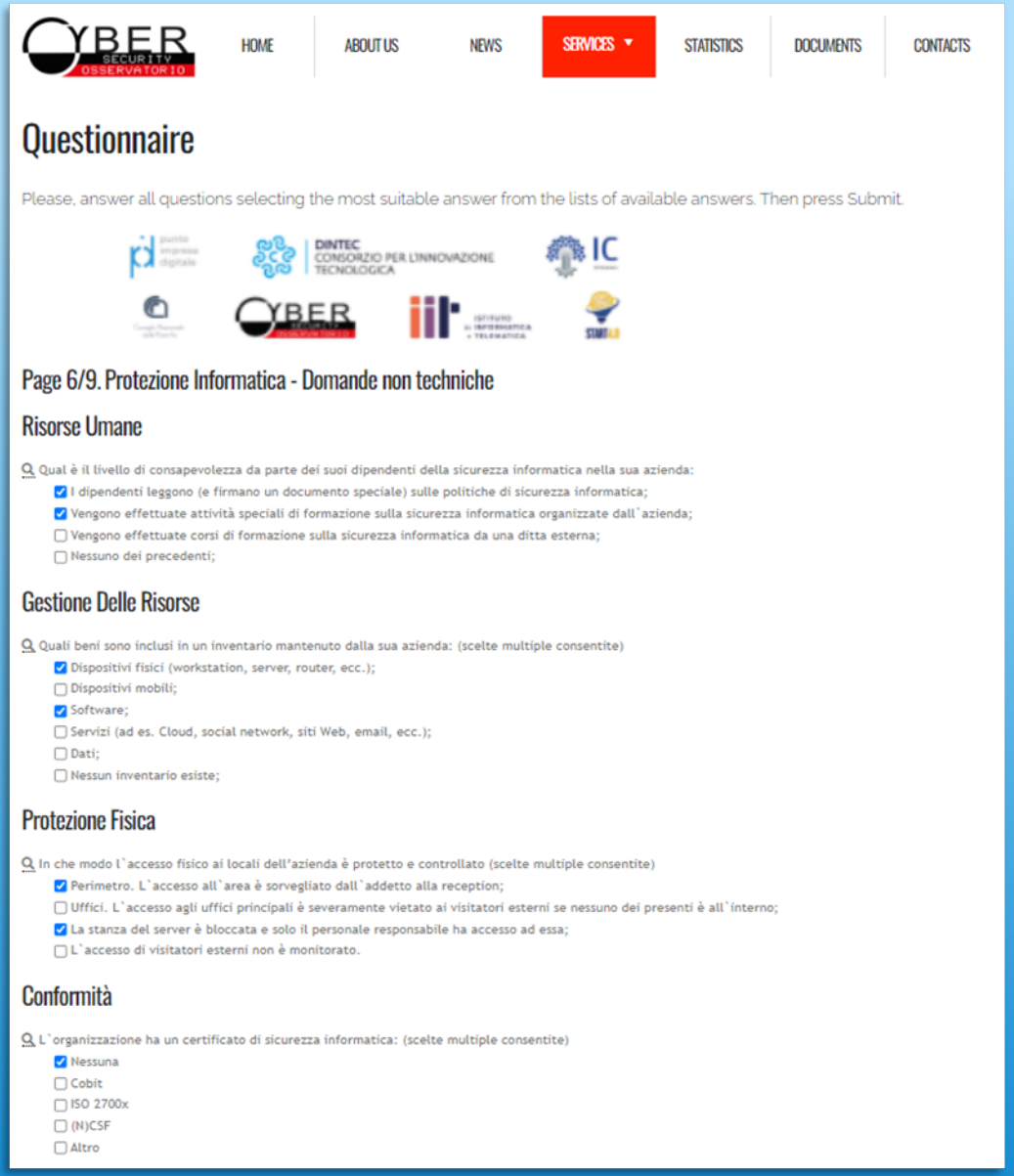
Consiglio Nazionale delle Ricerche

DESCRIZIONE DELL'IMPRESA E SUOI ASSETS

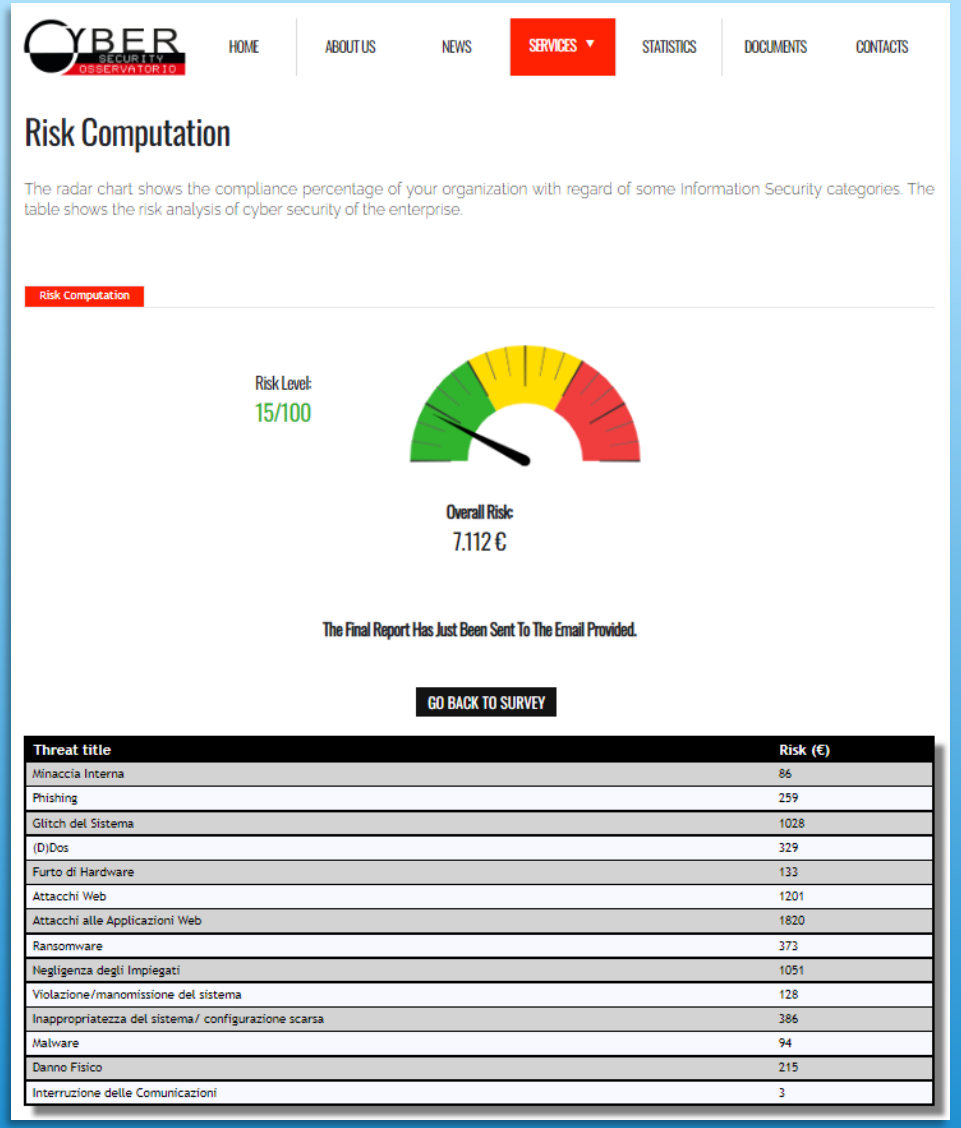




CONTROLLI DI SICUREZZA



RAPORTO FINALE



Threat title	Risk (€)
Minaccia Interna	86
Phishing	259
Glitch del Sistema	1028
(D)Dos	329
Furto di Hardware	133
Attacchi Web	1201
Attacchi alle Applicazioni Web	1820
Ransomware	373
Negligenza degli Impiegati	1051
Violazione/manomissione del sistema	128
Inappropriatezza del sistema/ configurazione scarsa	386
Malware	94
Danno Fisico	215
Interruzione delle Comunicazioni	3

Conclusioni

- Il PID Cyber Check e’ un facile strumento di self assessment
- Serve ad avere una idea della classe del livello di rischio attuale della vostra societa’ (autodiagnosi)
- Puo’ e deve essere utilizzato per verificare il miglioramento della propria postura di sicurezza.