



# 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 minacce anche e soprattutto 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



# 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*

”



# 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.

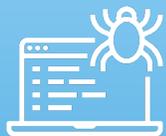
Molte infrastrutture critiche come il sistema energetico dipendono dalla sicurezza



# 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

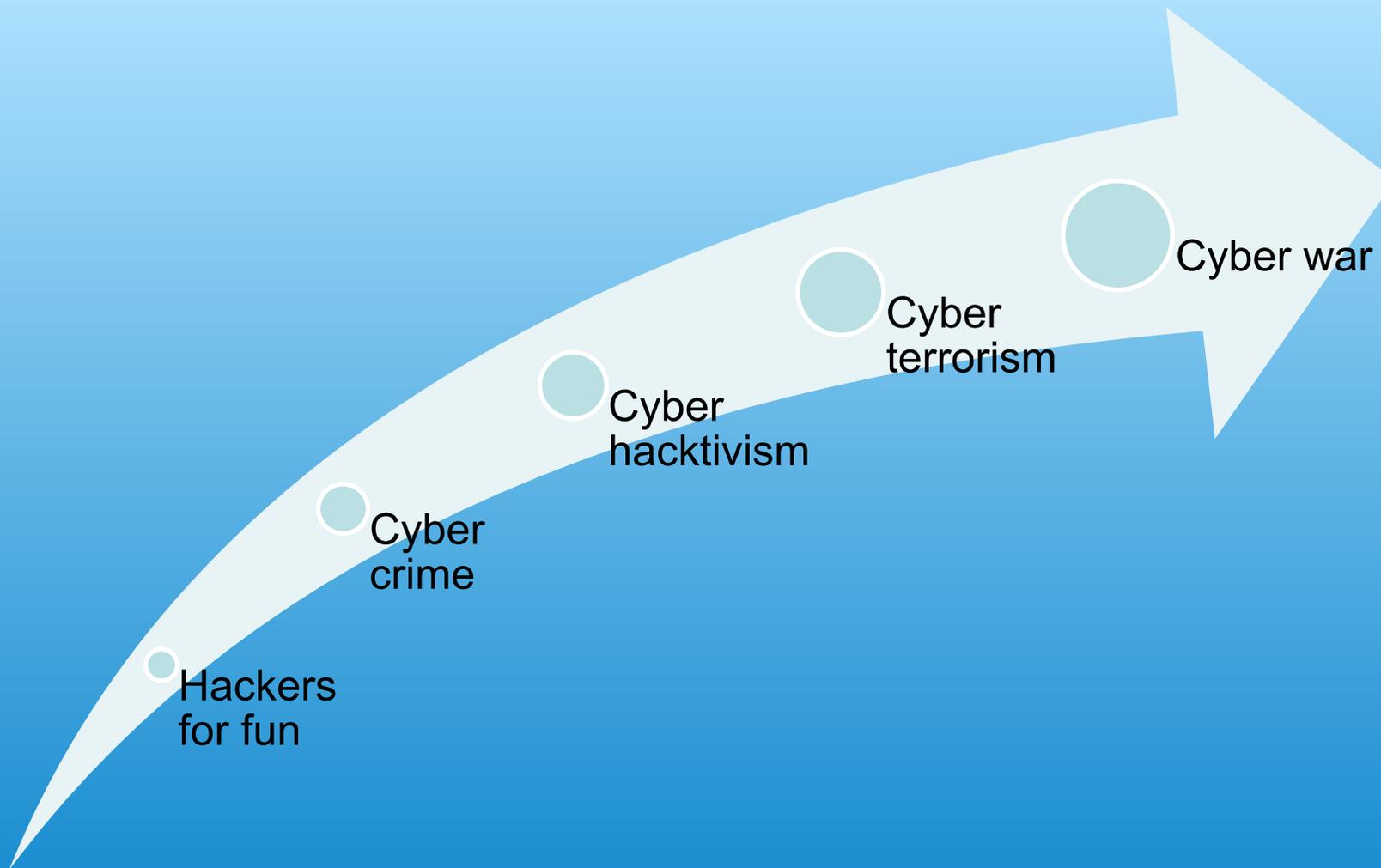


**MINACCIA (THREAT):**  
ENTITÀ/CIRCOSTANZA CHE PUÒ CAUSARE  
DANNI (ATTACCO, DISASTRO NATURALE, ...)

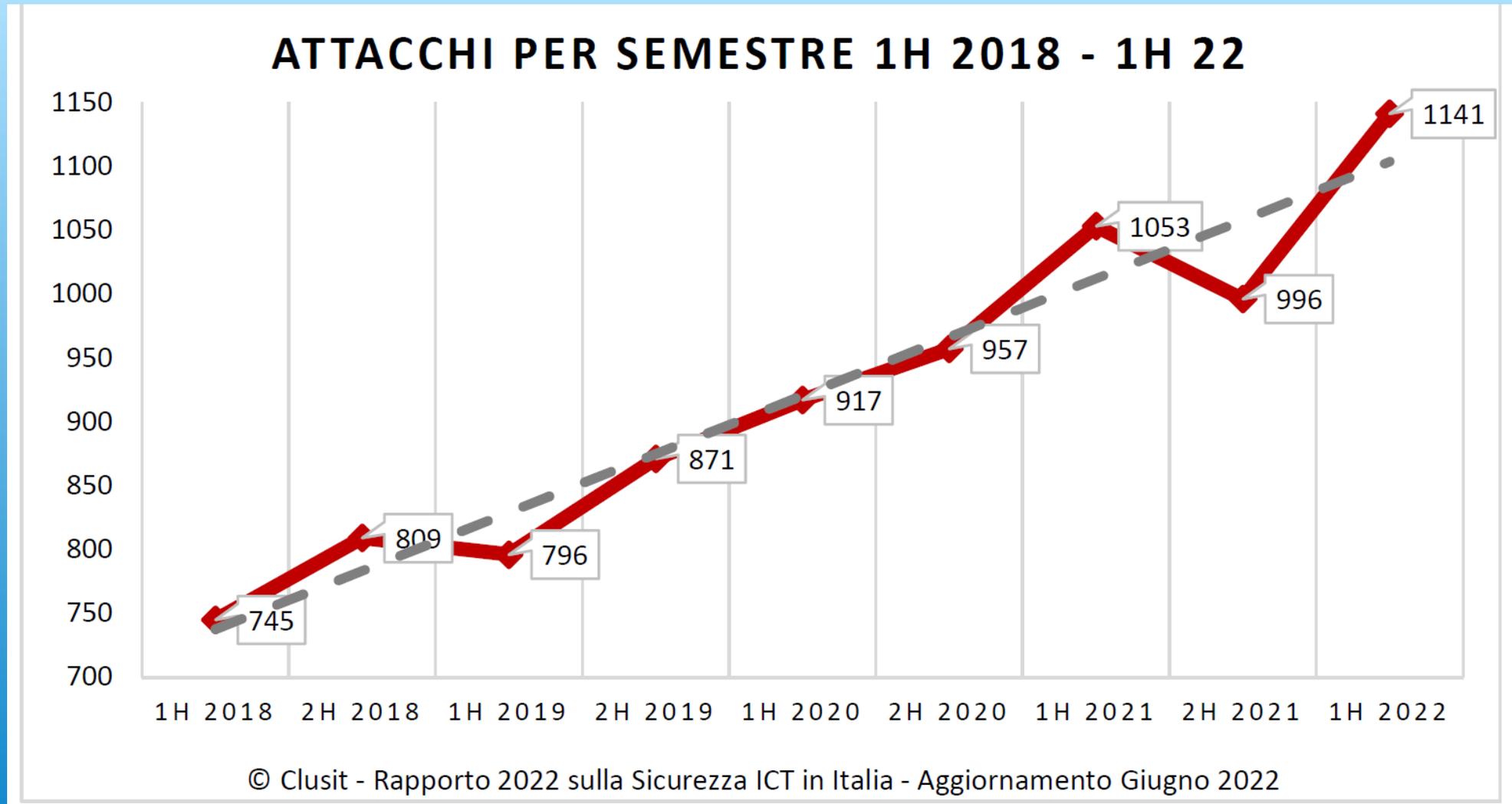
**CYBER SECURITY**



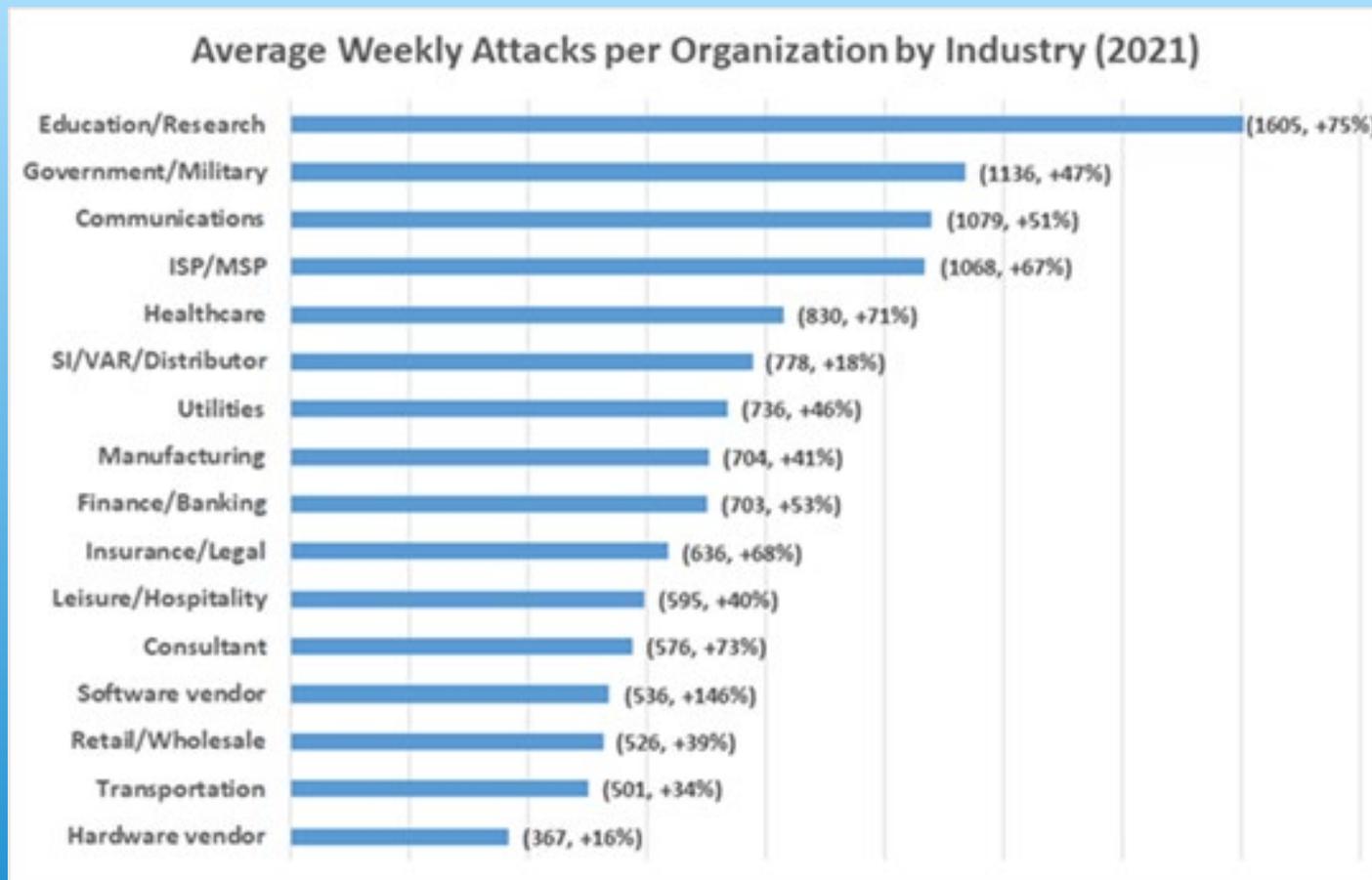
# Evoluzione delle minacce



# Crescita continua degli attacchi gravi



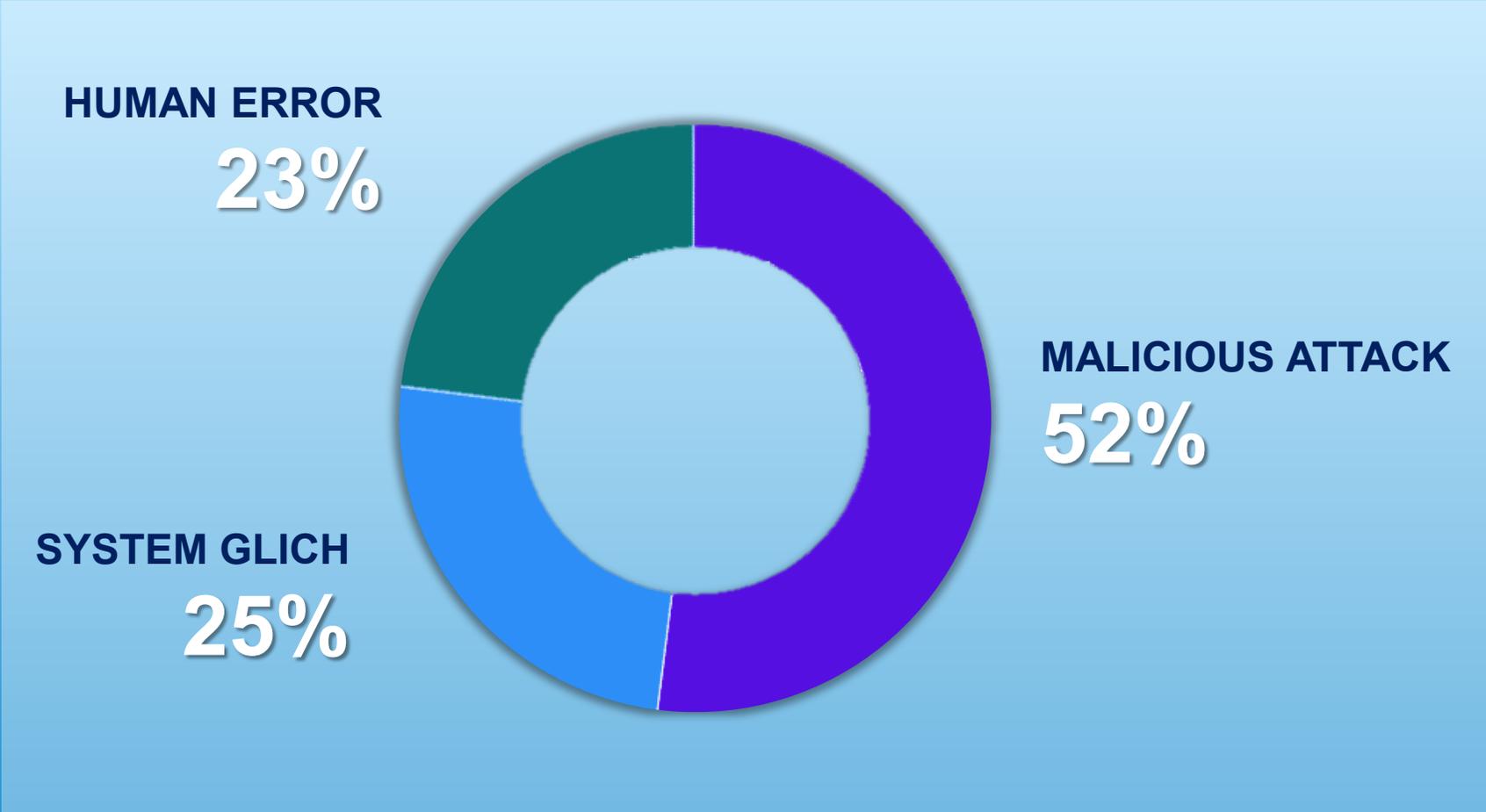
# Sectors



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

# DATA BREACHES/LEAKS

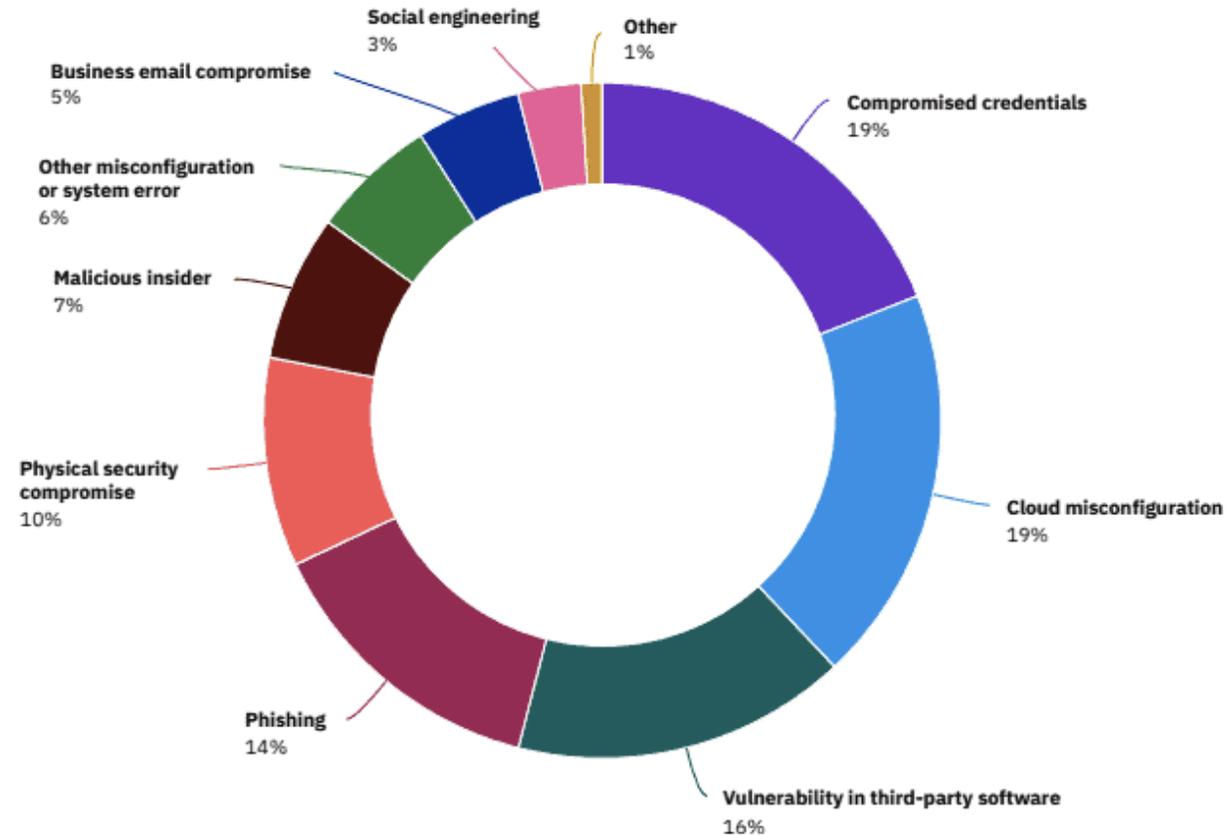
DATA BREACH ROOT COUSE BREAKDOWN IN THREE CATEGORIES



# Vettori di attacco per data breaches

Breakdown of malicious data breach root causes by threat vector

Percentage of breaches caused by malicious attack



# Tempo medio per rimediare ad un attacco

- 60 giorni nel 2022
- 40 giorni nel 2015

# Alcuni dati sul ransomware



**80%**

**VICTIMS OF RANSOMWARE ATTACK**  
THAT EXPERIENCED ANOTHER ATTACK SOON AFTER



**50%**

**HEALTHCARE DATA BREACHES**  
CAUSED BY RANSOMWARE ATTACKS



**46%**

**COMPANIES THAT ACCESSED THEIR**  
**DATA AFTER A RANSOMWARE**  
**ATTACK**

BUT FOUND THEM CORRUPTED



# 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

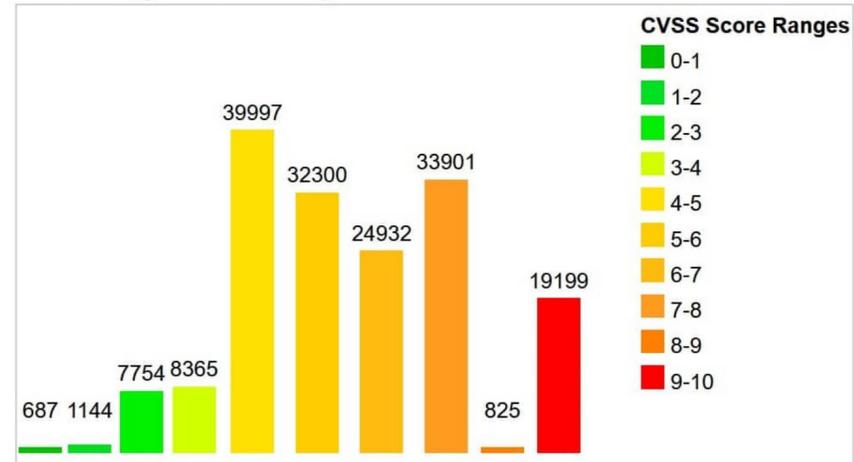
# Vulnerabilities

## Current CVSS Score Distribution For All Vulnerabilities

Distribution of all vulnerabilities by CVSS Scores

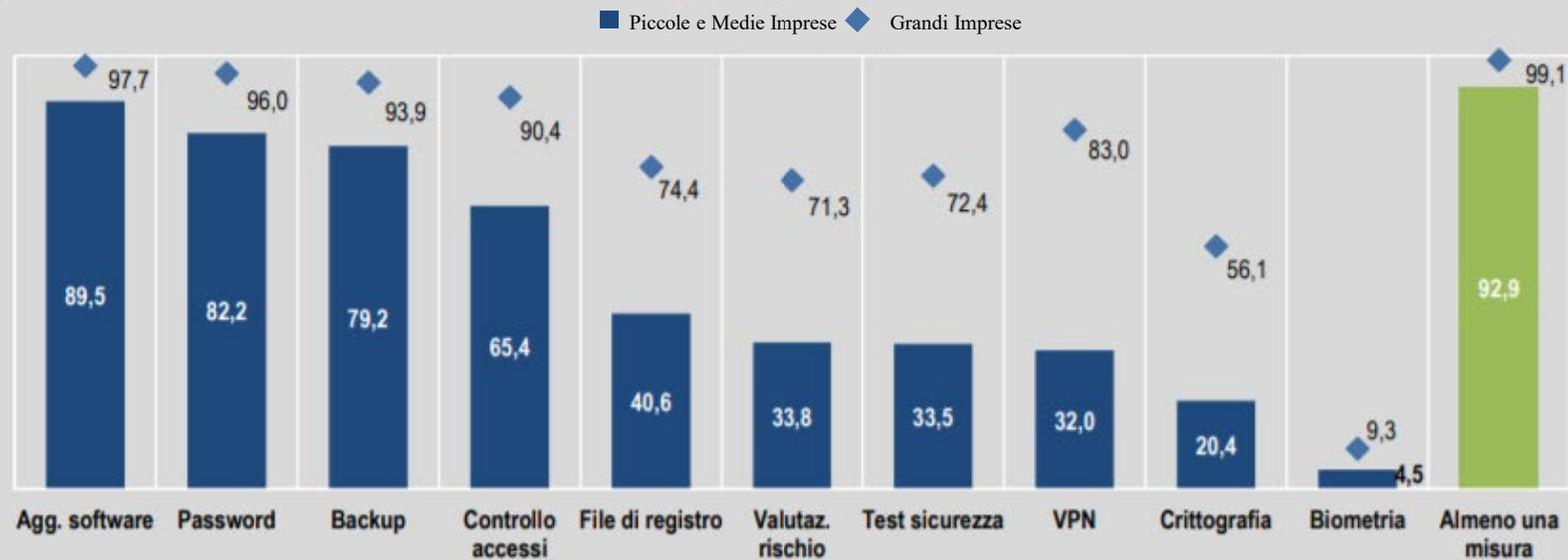
| CVSS Score   | Number Of Vulnerabilities | Percentage |
|--------------|---------------------------|------------|
| 0-1          | <a href="#">687</a>       | 0.40       |
| 1-2          | <a href="#">1144</a>      | 0.70       |
| 2-3          | <a href="#">7754</a>      | 4.60       |
| 3-4     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

Vulnerability Distribution By CVSS Scores



Weighted Average CVSS Score: **6.5**

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



# 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 <sup>(a)</sup> 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

# 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   |
| <b>Fonte: Rilevazione sulle tecnologie dell'informazione e della comunicazione nelle imprese, Anno 2019</b> |  |

|   | Imprese che effettuano test di sicurezza ICT |
|---|--|
| 10-49   | 30,6   |
| 50-99   | 49,1   |
| 100-249   | 58,4   |
| 250 e più   | 72,4   |
| <b>Fonte: Rilevazione sulle tecnologie dell'informazione e della comunicazione nelle imprese, Anno 2019</b> |  |

# Prontezza informatica di PMI

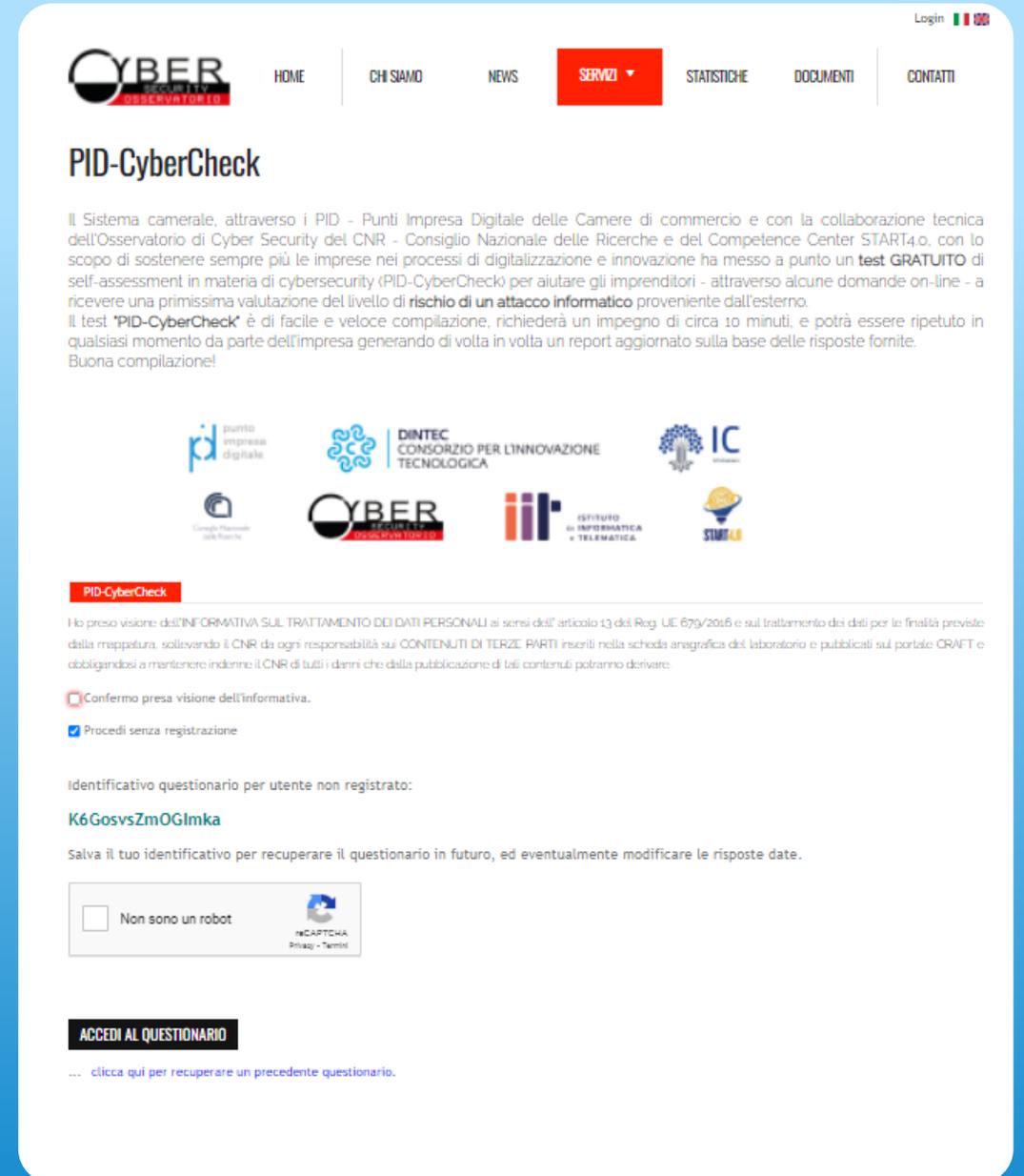
- Realta
  - L'85% delle violazioni dei dati colpisce le piccole imprese
  - Il 60% delle piccole imprese colpite da un attacco informatico si è spento entro sei mesi
  - le piccole e medie imprese stanno perdendo \$ 120.000 per incidente informatico
- risposta agli incidenti
  - Solo Il 54% non hanno un piano in atto per affrontare un attacco informatico
  - Altri Il 20% dicono che reagiranno 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.



The screenshot shows the PID-CyberCheck website. At the top, there is a navigation menu with links for HOME, CHI SIAMO, NEWS, SERVIZI (highlighted in red), STATISTICHE, DOCUMENTI, and CONTATTI. The main heading is "PID-CyberCheck". Below it, a paragraph explains the system's purpose: to assist businesses in digitalization and innovation through a free self-assessment tool. It mentions the involvement of the Italian Chamber of Commerce (Cassa di Risparmio di Roma) and the CNR Cyber Security Observatory. A list of partner logos follows, including "Punto Impresa Digitale", "DINTEC CONSORZIO PER L'INNOVAZIONE TECNOLOGICA", "IC", "Consiglio Nazionale delle Ricerche", "CYBER SECURITY OSSERVATORIO", "ISTITUTO DI INFORMATICA E TELEMATICA", and "SIMULA".

Below the logos, there is a section titled "PID-CyberCheck" with a privacy notice: "Ho preso visione dell'INFORMATIVA SUL TRATTAMENTO DEI DATI PERSONALI ai sensi dell' articolo 13 del Reg. UE 679/2016 e sul trattamento dei dati per le finalità previste dalla mappatura, sollevando il CNR da ogni responsabilità sui CONTENUTI DI TERZE PARTI inseriti nella scheda anagrafica del laboratorio e pubblicati sul portale CRAFT e obbligandomi a mantenere indenne il CNR di tutti i danni che della pubblicazione di tali contenuti potranno derivare."

There are two checkboxes: "Confermo presa visione dell'informativa." (unchecked) and "Procedi senza registrazione" (checked).

The user identification section shows "Identificativo questionario per utente non registrato: K6GosvsZmOGImka". Below this, it says "Salva il tuo identificativo per recuperare il questionario in futuro, ed eventualmente modificare le risposte date." and includes a "Non sono un robot" checkbox and a CAPTCHA widget.

At the bottom, there is a red button labeled "ACCEDI AL QUESTIONARIO" and a link: "... [clicca qui per recuperare un precedente questionario.](#)"

# PID CYBER CHECK - REPORT



## REPORT PER L'AZIENDA

ACME SPA

REDATTO IN BASE AI DATI FORNITI IL:

19 maggio 2022

CODICE PER RECUPERARE IL QUESTIONARIO:

twkj12093sdfj

Se il questionario è stato compilato senza registrazione, lo stringa qua sopra può essere utilizzato per recuperare le risposte ed eventualmente aggiornare/modificare



Pag. 1 a 5



### 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 risposte fornite al "PID-CyberCheck", il test di autovalutazione online del 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 cybersecurity da mettere in atto.

**RISCHIO ALTO** Un alto livello di rischio indica che l'impresa ha diverse criticità in tema di cybersecurity. Pertanto è fondamentale effettuare ulteriori approfondimenti, sottoponendo l'impresa a sistemi più approfonditi di analisi, e attuare interventi per ridurre il rischio cibernetico.



Pag. 2 a 5

CHECKUP  
Sicurezza IT



## LIVELLO DI RISCHIO



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.puntimpresa digitale.camcom.it](http://www.puntimpresa digitale.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 (€) | LEGENDA  |
|---------------------|-----------------------|--|
| Salvo di Valore     | 6.760                 | <b>Salvo di Valore</b> un problema tecnologico (ad esempio, un problema di integrazione o una funzionalità di segnalazione degli errori) che compromette la sicurezza informatica.   |
| Phishing            | 10.720                | <b>Phishing</b> è un "social engineering" (inganno) simulato con un'email o un messaggio di testo che sembra legittimo ma che serve a rubare informazioni o a installare malware.  |
| Furto di Hardware   | 1.300                 | <b>Furto di Hardware</b> è un furto fisico di apparecchiature, che possono contenere informazioni importanti o essere essenziali per la fornitura del servizio.  |
| Attacco DDoS        | 12.760                | <b>Attacco DDoS</b> è un attacco che mira a rendere inaccessibile un servizio, sfruttando la vulnerabilità del sito computer. L'azione dell'attacco riduce il servizio anche per molto tempo e può far perdere dati e compromettere la reputazione del servizio. |
| Denegazione         | 11.000                | <b>Denegazione</b> è un attacco che mira a rendere inaccessibile un servizio, sfruttando la vulnerabilità di un servizio o di un sito Web per interrompere, rendere inaccessibile o danneggiare i dati del servizio.   |
| Rischio Complessivo | 30.310                | <b>Denegazione</b> è un attacco che mira a rendere inaccessibile un servizio, sfruttando la vulnerabilità di un servizio o di un sito Web per interrompere, rendere inaccessibile o danneggiare i dati del servizio.   |

## QUANTIFICAZIONE DEL RISCHIO



Pag. 3 a 5



Pag. 4 a 5



Pag. 5 a 5



# DESCRIZIONE DELL'IMPRESA E SUOI ASSETS

**Questionnaire**

Please, answer all questions selecting the most suitable answer from the lists of available answers. Then press Submit.

paesie imprese digitale | DINTEC CONSORZIO PER L'INNOVAZIONE TECNOLOGICA | IC | CYBER SECURITY OBSERVATORIO | ISTITUTO DI INFORMATICA E TELEMATICA | SIMUL

### Page 1/9. Informazioni sull'organizzazione

Ragione Sociale  
Italy

CF/Partita IVA  
Pisa

Provincia  
Pisa

Email di contatto  
test@it.cnr.it

Settore:

- Servizi Amministrativi e di Supporto
- Trasporto e Deposito
- Centro di Ricerca o Altamente Specializzato
- Educazione
- Alimentazione, Alloggio, Viaggi
- Servizi di Base
- Elettricità e gas
- Costruzioni
- Manifatturiero
- Gestionale
- Agenzie Immobiliari
- Informazione e Comunicazione
- Servizi Finanziari
- Al dettaglio
- Assistenza sanitaria
- Amministrazione Pubbico
- Altro

Turnover:

- >20 milioni per anno
- 10-20 milioni per anno
- 2-10 milioni per anno

**Questionnaire**

Please, answer all questions selecting the most suitable answer from the lists of available answers. Then press Submit.

paesie imprese digitale | DINTEC CONSORZIO PER L'INNOVAZIONE TECNOLOGICA | IC | CYBER SECURITY OBSERVATORIO | ISTITUTO DI INFORMATICA E TELEMATICA | SIMUL

### Page 3/9. Informazioni sulle risorse dati

Quali dei seguenti dati sono memorizzati dalla vostra azienda (sono consentite risposte multiple):

Informazioni del cliente:

- Informazioni sanitarie personali (stato di salute, storia delle malattie, prescrizioni, ecc.);
- Informazioni personali identificabili (nome, codice fiscale, indirizzo, sesso, ecc.);
- Informazioni finanziarie (dettagli delle carte di credito, cronologia degli acquisti, ecc.);
- Nessuno dei precedenti;

Something else? Insert the information in the text fields below

Informazioni di altre aziende partner:

- Record finanziari;
- Know-how;
- Informazioni sulle transazioni;
- Informazioni sui clienti del partner.
- Nessuno dei precedenti;

Something else? Insert the information in the text fields below

Informazioni dell'azienda:

- Informazioni finanziarie;
- Dati operativi;
- Know-how;
- Informazioni su transizioni;
- Audit e Log;
- Media;
- Nessuno dei precedenti;

Something else? Insert the information in the text fields below

HOME ABOUT US NEWS SERVICES STATISTICS DOCUMENTS CONTACTS

## Questionnaire

Please, answer all questions selecting the most suitable answer from the lists of available answers. Then press Submit.



### Page 6/9. Protezione Informatica - Domande non tecniche

#### Risorse Umane

Qual è il livello di consapevolezza da parte dei suoi dipendenti della sicurezza informatica nella sua azienda:

- I dipendenti leggono (e firmano un documento speciale) sulle politiche di sicurezza informatica;
- Vengono effettuate attività speciali di formazione sulla sicurezza informatica organizzate dall'azienda;
- Vengono effettuate corsi di formazione sulla sicurezza informatica da una ditta esterna;
- Nessuno dei precedenti;

#### Gestione Delle Risorse

Quali beni sono inclusi in un inventario mantenuto dalla sua azienda: (scelte multiple consentite)

- Dispositivi fisici (workstation, server, router, ecc.);
- Dispositivi mobili;
- Software;
- Servizi (ad es. Cloud, social network, siti Web, email, ecc.);
- Dati;
- Nessun inventario esiste;

#### Protezione Fisica

In che modo l'accesso fisico ai locali dell'azienda è protetto e controllato (scelte multiple consentite)

- Perimetro. L'accesso all'area è sorvegliato dall'addetto alla reception;
- Uffici. L'accesso agli uffici principali è severamente vietato ai visitatori esterni se nessuno dei presenti è all'interno;
- La stanza del server è bloccata e solo il personale responsabile ha accesso ad essa;
- L'accesso di visitatori esterni non è monitorato.

#### Conformità

L'organizzazione ha un certificato di sicurezza informatica: (scelte multiple consentite)

- Nessuna
- Cobit
- ISO 2700x
- (N)CSF
- Altro



Consiglio Nazionale  
delle Ricerche

The screenshot shows a web page titled "Risk Computation" from the Cyber Security Observatory. The page features a navigation menu with links for HOME, ABOUT US, NEWS, SERVICES (highlighted in red), STATISTICS, DOCUMENTS, and CONTACTS. Below the title, a paragraph explains that a radar chart shows compliance percentages and a table shows risk analysis. The radar chart displays a "Risk Level: 15/100" and an "Overall Risk: 7.112 €". A message states "The Final Report Has Just Been Sent To The Email Provided." with a "GO BACK TO SURVEY" button. At the bottom, a table lists various threat titles and their corresponding risk values in Euros.

| 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.