



# CYBERSECURITY

*LA SICUREZZA IT PER LE PMI  
E IL PID CYBER CHECK*

Consiglio Nazionale delle Ricerche (CNR)

***Cybersecurityosservatorio.it***



Consiglio Nazionale  
delle Ricerche



# DUE PAROLE SULLA MIA ORGANIZZAZIONE

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

# LABORATORIO VIRTUALE CYBER SECURITY DEL CNR

## RICERCATORI DI VARI ISTITUTI/SEDI COINVOLTI:

- ✓ IAC – Napoli
- ✓ IAC – Roma
- ✓ ICAR – Cosenza
- ✓ ICAR - Napoli
- ✓ IEIT – Torino
- ✓ IEIT – Genova
- ✓ IIT - Pisa
- ✓ IMATI – Genova
- ✓ IMATI – Milano
- ✓ INO - Firenze
- ✓ IRCRES – Torino
- ✓ ISTC – Roma
- ✓ ISTI - Pisa
- ✓ ITAE - Messina
- ✓ ...



# 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

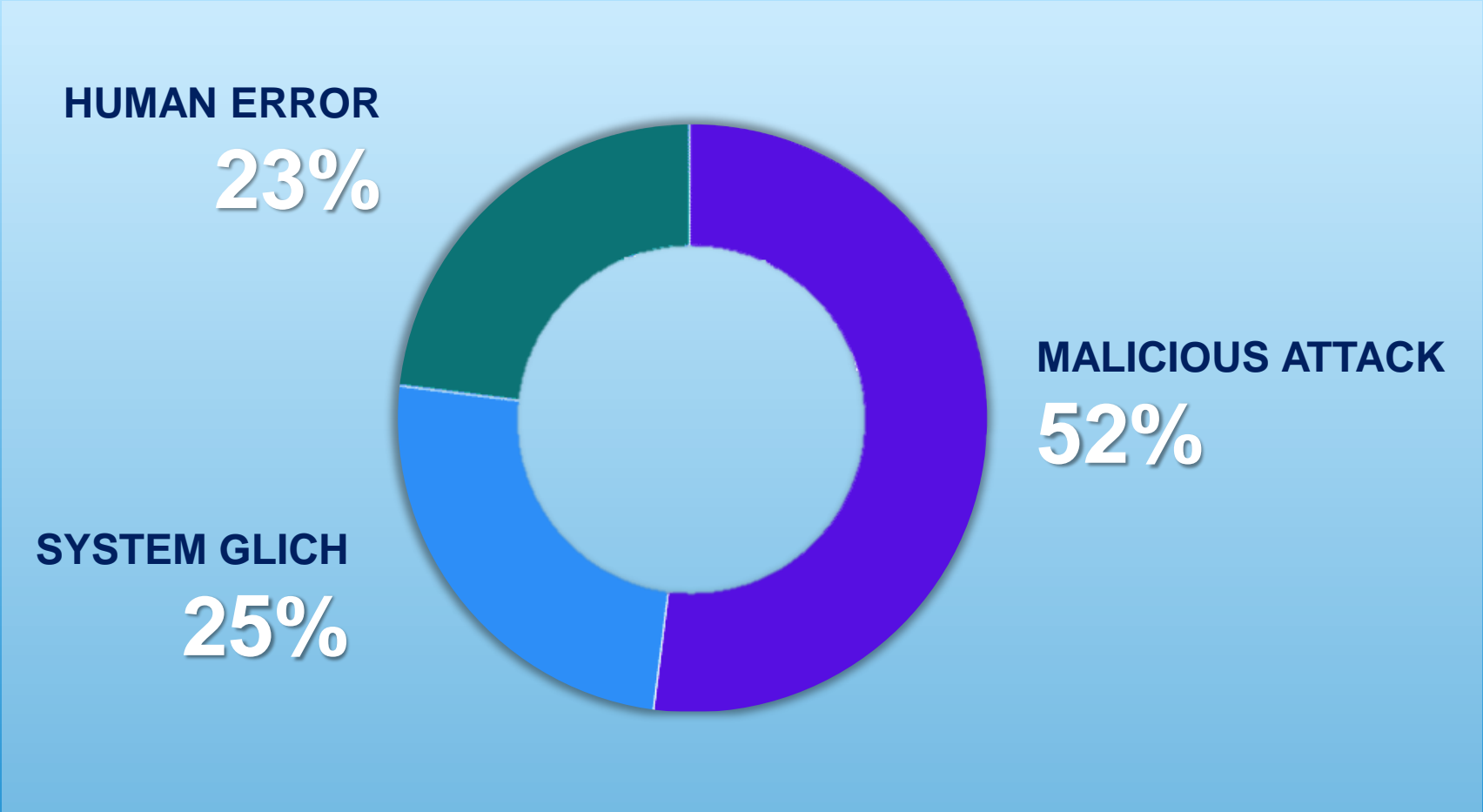


**MINACCIA (THREAT):**  
ENTITÀ/CIRCOSTANZA CHE PUÒ CAUSARE  
DANNI (ATTACCO, DISASTRO NATURALE, ...)

CYBER SECURITY

# DATA BREACHES/LEAKS

DATA BREACH ROOT COUSE BREAKDOWN IN THREE CATEGORIES



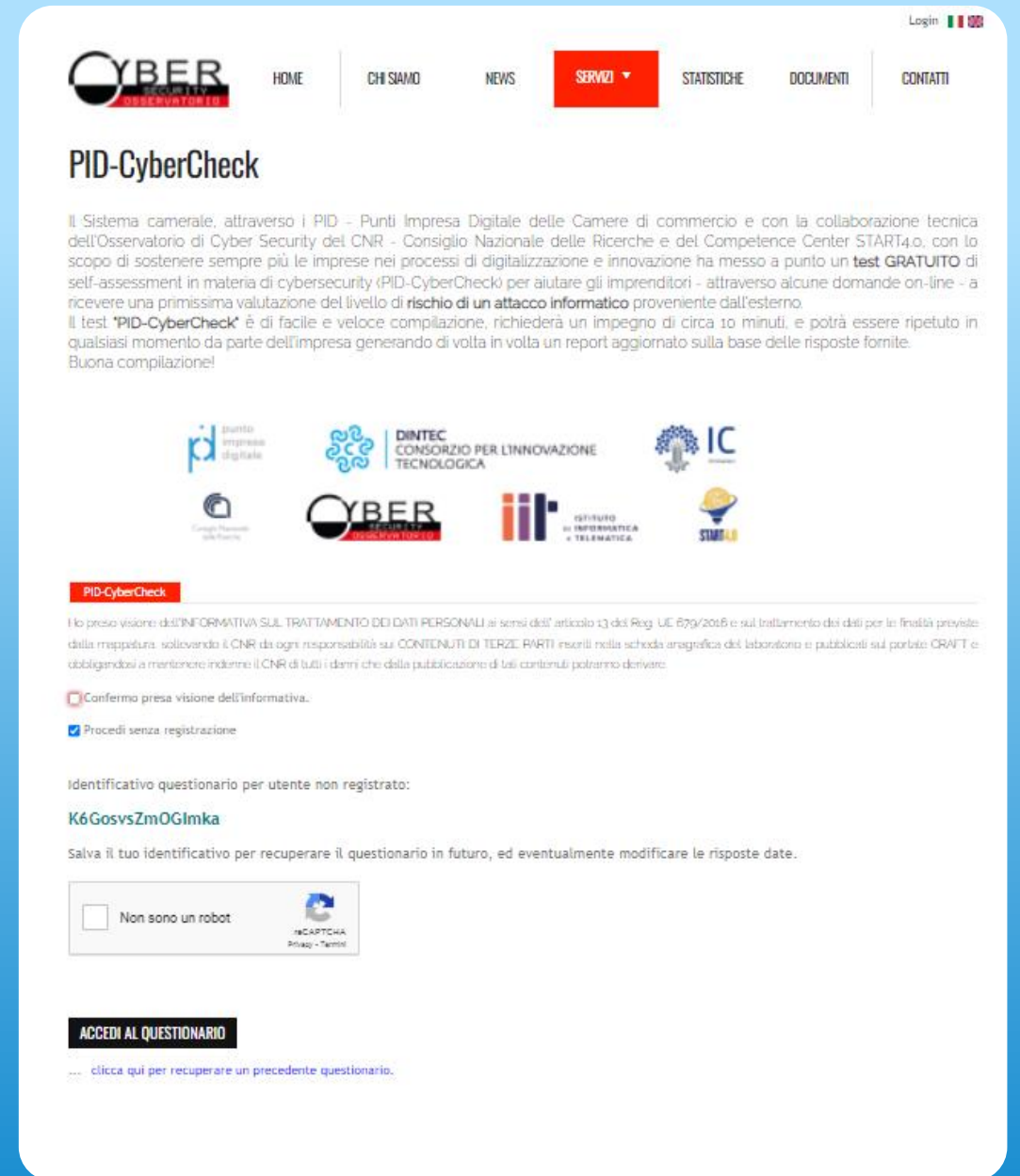
<https://www.metacompliance.com/blog/calculating-the-heavy-cost-of-data-breaches-in-2021/>

# **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 help businesses assess their cybersecurity risks through a free self-assessment tool. It mentions collaboration with the CNR Cyber Security Observatory and the START4.0 center. The text states that the test is quick (around 10 minutes) and can be repeated at any time. Below the text, there are logos for partner organizations: Puntino Impresa Digitale, DITEC (Consorzio per l'Innovazione Tecnologica), IC, Consiglio Nazionale delle Ricerche, CYBER SECURITY OSSERVATORIO, IIT (Istituto di Informatica e Telematica), and SIMEL. A red button labeled "PID-CyberCheck" is visible. Below the button, there is a privacy notice and two checkboxes: "Confermo presa visione dell'informativa." (unchecked) and "Procedi senza registrazione" (checked). A unique identifier "K6GosvsZmOGImka" is displayed. Below this, there is a text prompt to save the identifier for future use. A reCAPTCHA widget is present with the text "Non sono un robot". At the bottom, there is a black button labeled "ACCEDI AL QUESTIONARIO" and a link to recover a previous questionnaire.



# 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:

twkij12093sdfj

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



Pag. 1 di 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 di 5

## 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 lo potete trovare al seguente link: [www.puntoimpresa-digitale.camcom.it](http://www.puntoimpresa-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
Cloud/CRM	4.700	<b>Cloud/CRM</b> : un problema tecnologico (ad esempio, un problema di integrazione o una funzionalità di segreteria degli email) che compromette la sicurezza informatica.
Phishing	10.000	<b>Phishing</b> : minaccia "social-engineering" il cliente malintenzionato con un enorme quantità di richieste che rendono il servizio non disponibile per gli utenti legittimi.
Furto di Hardware	1.300	<b>Furto di Hardware</b> : Furto fisico di apparecchiature, che possono contenere informazioni importanti o essere sensibili per la funzionalità del servizio.
Attacco Web	12.700	<b>Attacco Web</b> : questa minaccia prevede di uno gli utenti del servizio, affidando e sfruttando le vulnerabilità dei loro computer. L'autore dell'attacco sfrutta un servizio web per mettere a nudo le vulnerabilità dei browser e di far eseguire il proprio codice.
Denegazione	11.000	<b>Denegazione</b> : l'attacco a un sito web o a un sito per interferire con la vulnerabilità di un servizio o di un sito web per interferire con la funzionalità del servizio e accedere a dati sensibili.
Rischio Complessivo	38.115	<b>Denegazione</b> : l'attacco a un sito web o a un sito per interferire con la vulnerabilità di un servizio o di un sito per interferire con la funzionalità del servizio e accedere a dati sensibili.

## QUANTIFICAZIONE DEL RISCHIO



Pag. 3 di 5



Pag. 4 di 5



Pag. 5 di 5



Consiglio Nazionale delle Ricerche

# 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.

giustizia imprese digitale | DINTEC CONSORZIO PER L'INNOVAZIONE TECNOLOGICA | IC | Cyber Security | CYBER | 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.

giustizia imprese digitale | DINTEC CONSORZIO PER L'INNOVAZIONE TECNOLOGICA | IC | Cyber Security | CYBER | 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


HOME ABOUT US NEWS SERVICES STATISTICS DOCUMENTS CONTACTS

## Risk Computation

The radar chart shows the compliance percentage of your organization with regard of some Information Security categories. The table shows the risk analysis of cyber security of the enterprise.

Risk Computation

Risk Level:  
15/100



Overall Risk:  
7.112 €

The Final Report Has Just Been Sent To The Email Provided.

[GO BACK TO SURVEY](#)

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

“

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

”

