




QUANTO SEI

CYBER READY?

Servizio CYBER 2025

FPI FONDAZIONE
PIEMONTE
INNOVA

cyber@piemonteinnova.it 

www.piemonteinnova.it 

Indice

[Il contesto](#)

[Gli enti a supporto](#)

[La nostra soluzione](#)

[Information e cybersecurity BASE](#)

[Information e cybersecurity AVANZATA](#)

[Offerta avanzata](#)

[Offerta base+avanzata](#)

[Il team](#)

[Contatti](#)

"How you gather, manage, and use information will determine whether you win or lose." Bill Gates

Il contesto

Il panorama di riferimento per il **rischio cyber** sta vivendo un momento di grande turbolenza, caratterizzato da un **aumento considerevole degli attacchi**.

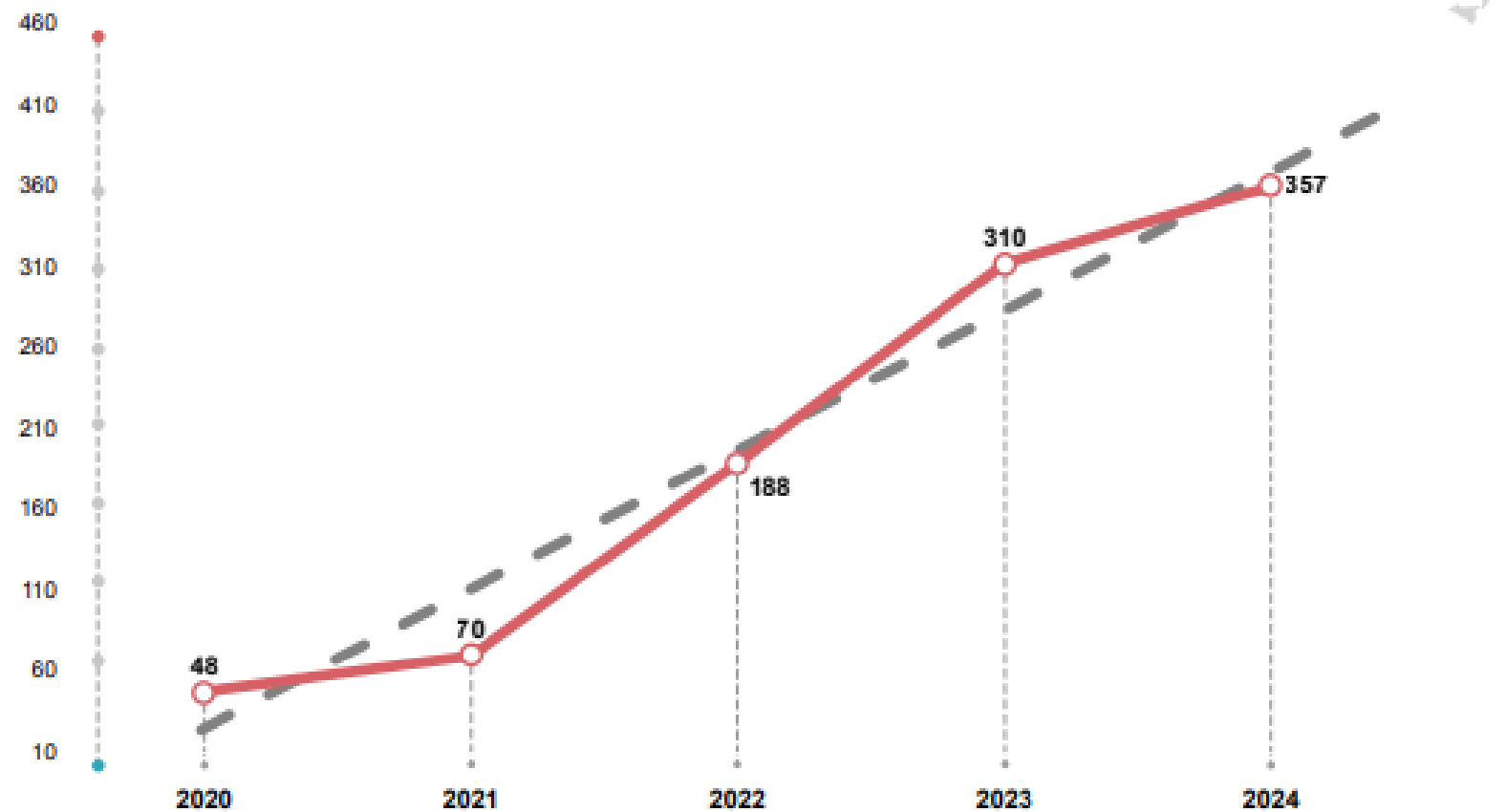
The screenshot shows a webpage from CYBERSECURITY360. The main headline is "Più cyber attacchi nel 2024. E nel 2025 il trend non si fermerà". Below the headline, there is a sub-headline: "I report di livello Europeo forniti da ENISA e quelli centrati sull'Italia aiutano a comprendere lo scenario della minaccia, nel lasso temporale che va dal 2023 ad oggi, con uno sguardo sul futuro prossimo". The article was published on January 22, 2025. The page also features a search bar, navigation tabs for "Cybersecurity Nazionale", "Malware e attacchi", and "Norme e adeguamenti", and social media sharing icons for Facebook, LinkedIn, X, Email, Print, and a link icon.

Il **cybercrime** è una **minaccia** con impatti sia sull'infrastruttura digitale che su:



Evoluzione degli Attacchi ICT in Italia e nel mondo 2024

Incidenti Cyber in Italia 2020 -2024

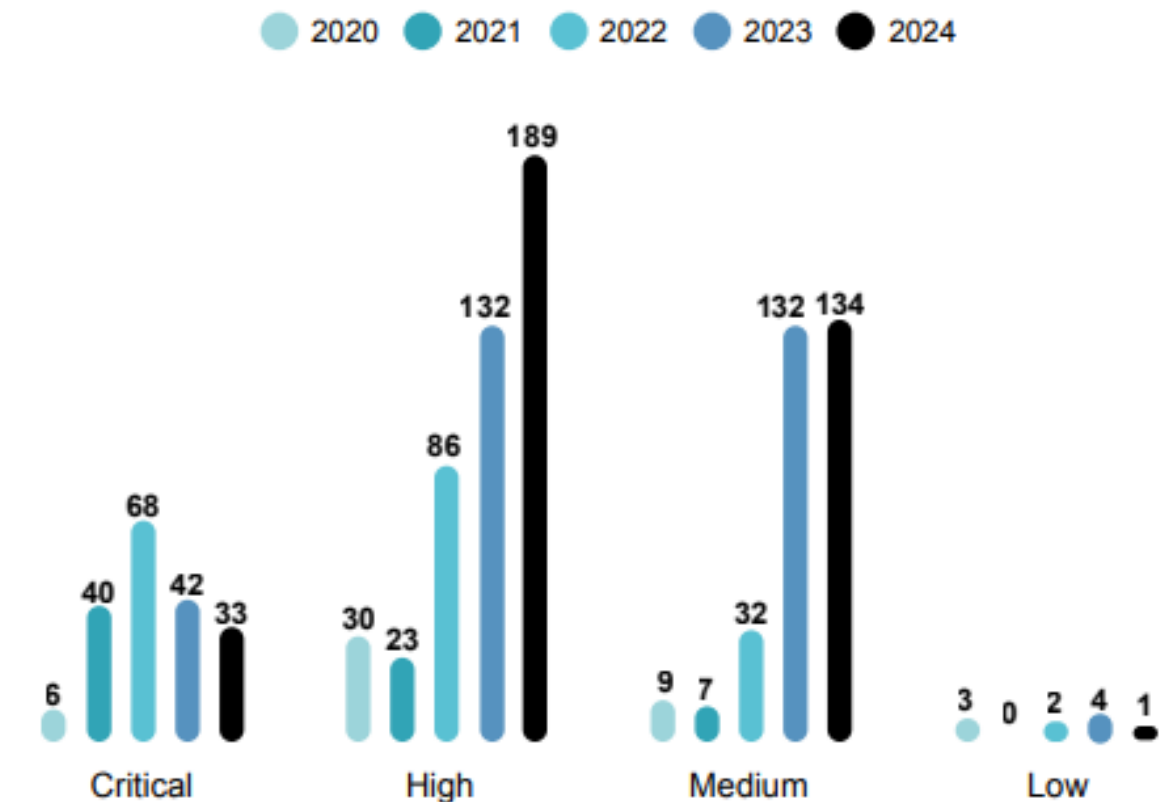


© Clusit - Rapporto 2025 sulla Cybersecurity

357 incidenti noti in Italia

39% del totale

Severity in Italia 2020 - 2024



© Clusit - Rapporto 2025 sulla Cybersecurity

Fig. 33 - Severity degli attacchi in Italia nel periodo 2020-2024

198 incidenti high severity in Italia nel 2024

Crescita +10% rispetto 2023

Impatto del ransomware sui fatturati

Secondo una recente indagine* che ha coinvolto circa **200 security manager** operanti in aziende di oltre **20 settori**, con un fatturato complessivo superiore ai **700 miliardi di euro**, il **beneficio atteso** cambia in funzione della **dimensione aziendale**.

Il **ransomware** è il **principale fattore di rischio** per le imprese con **fatturato inferiore a 1 miliardo di euro l'anno**, ma l'incidenza dei danni che può provocare è esponenziale a seconda del fatturato:

- **55 mila euro** sulle realtà con fatturato **fino a 50 milioni** di euro l'anno;
- **900 mila euro** per chi fattura **fino a 250 milioni** l'anno;
- **7,8 milioni di euro** per fatturati **fino a 1 miliardo** l'anno.



*Osservatorio Security Risk condotto da AIPSA E TEHA

Conviene investire nel rischio?

Secondo una recente indagine* che ha coinvolto circa **200 security manager** operanti in aziende di oltre **20 settori**, con un fatturato complessivo superiore ai 700 miliardi di euro, il beneficio atteso cambia in funzione della dimensione aziendale.

Riduzione del rischio di un attacco ransomware

Per un'azienda tra i **50 e 250 milioni di fatturato**, una riduzione del livello di rischio del 10%, si stima possa determinare un beneficio di circa **100.000 euro**.

Riduzione del livello di rischio della Supply Chain

Per un'azienda che fattura oltre **10 miliardi**, una **riduzione del 10% del rischio** che la supply chain subisca un attacco, si stima possa determinare un beneficio atteso di **oltre 30 milioni di euro**.



Come proteggersi? Gestire information e cybersecurity



Identificare il profilo di rischio in base al proprio business

Questo processo consente di comprendere quali aree aziendali sono più vulnerabili e come i rischi possono impattare le operazioni quotidiane.



Misurare il livello cybersecurity target da raggiungere in azienda

Impostare obiettivi chiari per la cybersecurity consente di determinare le risorse e gli investimenti necessari per implementare soluzioni efficaci.



Seguire le raccomandazioni pratiche immediate e di medio termine

Adottare misure preventive e correttive subito dopo aver identificato le vulnerabilità aiuta a ridurre il rischio di attacchi immediati.

Proteggere la cybersecurity è essenziale per la sicurezza aziendale. Ecco i primi passi per gestire il rischio e garantire la protezione delle informazioni.



Come proteggersi? Gestire information e cybersecurity



Promuovere internamente e lungo la filiera la Data Protection

Incorporare la protezione dei dati nella cultura aziendale e lungo la supply chain è cruciale per ridurre i rischi legati alla sicurezza delle informazioni.



Lavorare sulla sicurezza delle informazioni secondo lo standard ISO/IEC 27001*

Adottare standard riconosciuti a livello internazionale, come l'ISO/IEC 27001, assicura una gestione della sicurezza delle informazioni conforme e di alta qualità.



Investire in formazione mirata per i dipendenti per una crescita di consapevolezza

La formazione continua permette ai dipendenti di riconoscere le minacce informatiche e adottare comportamenti sicuri.

Promuovere la cultura della protezione dei dati, seguire gli standard internazionali e investire nella formazione continua sono ulteriori passi fondamentali per garantire una protezione duratura e sicura delle informazioni aziendali.



Gli enti a supporto della tua impresa



Fondazione Piemonte Innova è un partenariato pubblico-privato che **abilita l'innovazione e la digitalizzazione delle imprese e delle organizzazioni no-profit**, affiancando le pubbliche amministrazioni per lo sviluppo di progetti di innovazione, sostenibili e replicabili.



Il Centro di Competenza START 4.0 per la sicurezza e l'ottimizzazione delle infrastrutture strategiche è un partenariato pubblico-privato e rappresenta uno strumento che **incentiva la crescita della maturità digitale del sistema economico italiano** e supporta l'adozione nelle imprese di nuove tecnologie.

FPI e START4.0 sono due realtà senza scopo di lucro e il **supporto è esclusivamente mirato alla crescita di consapevolezza sui temi della cybersecurity all'interno delle imprese, in particolare delle PMI.**

Come enti terzi offrono il sostegno a comprendere se l'impresa gestisce correttamente i processi legati alla cybersecurity e lavorano **al fianco di amministratori e manager per implementare soluzioni concrete** per una corretta gestione delle attività interne e per lo sviluppo delle competenze del personale.

La nostra soluzione per la tua impresa

CYBER BASE

- Analisi base della situazione aziendale
- Consapevolezza Cyber
- Percorso di crescita delle competenze (5 Moduli di formazione)

CYBER AVANZATA

- Percorso di crescita delle competenze (3 Moduli di formazione specifici)
- Casi studio
- Cyber Incident Response Experience
- Re-check della situazione aziendale



INFORMATION E CYBER SECURITY BASE

Servizio CYBER 2025

FPI FONDAZIONE
PIEMONTE
INNOVA

cyber@piemonteinnova.it

www.piemonteinnova.it 

La nostra proposta

Cybersecurity **base**

ANALISI SITUAZIONE AZIENDALE



- Identificazione profilo di rischio cyber
- misurazione del livello target
- raccomandazioni pratiche

CONSAPEVOLEZZA CYBER



Sensibilizzazione diffusa:

- Approccio alla Cybersecurity Dati e privacy
- Cyberwarfare

CRESCITA COMPETENZE



5 moduli di tre ore per sviluppare competenze specifiche e gestire:

- persone
- processi
- tecnologie

Analisi base della situazione aziendale



IL TOOL

Il **CYBER ASSESSMENT** viene effettuato attraverso un **tool** sviluppato congiuntamente da **Fondazione Piemonte Innova**, dai Competence Center Nazionali **Cyber4.0** e **Start4.0**, dai **Digital Innovation Hub** di **Liguria** e **Piemonte**, su mandato di **Confindustria**.



L'OBBIETTIVO

Il **CYBER ASSESSMENT** punta ad **aumentare la consapevolezza dell'impresa sul tema cyber** e a fornire una **fotografia del livello di maturità cyber** basata su standard di riferimento nazionali e internazionali. L'azienda potrà migliorare la propria postura cyber grazie alle **azioni di remediation** fornite.



I RIFERIMENTI

Il **CYBER ASSESSMENT** si basa sui riferimenti del **Framework nazionale per la Cybersecurity e Data Protection (FNCS)** e dello standard internazionale **ISO/IEC 27001**. L'Assessment è strutturato su 13 Category che analizzano il business aziendale in merito a processi, persone e tecnologie.

Analisi base della situazione aziendale

Il processo



INDIVIDUAZIONE PROFILI DI RISCHIO

Lo strumento individua il profilo target da raggiungere.

IL **CYBER ASSESSMENT** SI ADATTA ALLO SPECIFICO CONTESTO



MISURAZIONE DEL LIVELLO CYBER

Lo strumento misura il livello e indica se il target è superato o meno.

IL **CYBER ASSESSMENT** FORNISCE POSTURA DI SICUREZZA DELL'ORGANIZZAZIONE



SUGGERIMENTI PRATICI

Lo strumento suggerisce azioni per superare il livello target

IL **CYBER ASSESSMENT** AIUTA A IMPLEMENTARE UNA ROADMAP DI REMEDIATION

Consapevolezza Cyber



CYBERSECURITY

- Cenni storici
- Definizione e principi cardine
- Cybercrime (tipologie e reati)
- Criminali informatici (tipologie e caratteristiche)
- Attacchi informatici e casi reali



DATI E PRIVACY

- Raccolta e condivisione dati
- Violazioni privacy e conseguenze
- Panoramica normativa (GDPR)
- Responsabilità delle aziende
- Protezione privacy online



CYBERWARFAR E

- Panoramica del fenomeno e caratteristiche
- Casi reali
- Ripercussioni e connessioni con la Supply Chain
- Misure di protezione

Percorso di crescita delle competenze - BASE



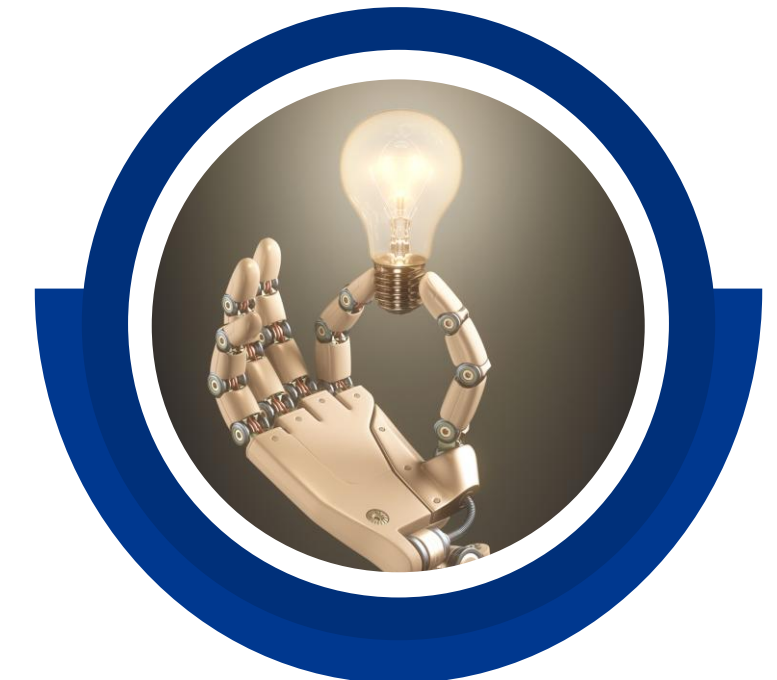
PERSONE

- Focus vulnerabilità "Fattore Umano"
- Focus attacchi di Ingegneria Sociale
- Casi reali di attacchi cyber
- Consigli e azioni di immediata applicazione



PROCESSI E NORMATIVE

- Processi in ottica di risposta agli incidenti
- Gestione continuità operative
- Panoramica normative cybersecurity nazionali e internazionali (NIS II, ISO/IEC 27001)



TECNOLOGIE

- Identità digitali e accessi
- Processi di autenticazione e autorizzazione
- Perimetro sicurezza e superfici di attacco
- Sicurezza di rete

Offerta base

	PICCOLA IMPRESA	MEDIA IMPRESA	GRANDE IMPRESA
Valore della proposta	4.400 € + IVA	5.500 € + IVA	8.800 € + IVA
Finanziamento	80%	70%	40%
Quota a carico	880 € + IVA*	1.650 € + IVA*	5.280 € + IVA*

INFORMATION E CYBER SECURITY AVANZATA

Servizio CYBER 2025

FPI FONDAZIONE
PIEMONTE
INNOVA

cyber@piemonteinnova.it

www.piemonteinnova.it 

La nostra proposta

Cybersecurity **avanzata**



1 Crescita competenze

3 moduli di tre ore per approfondire tematiche specifiche: Gdpr, Nis II e Iso/lec 27001



2 Casi studio

Business Case reali per:

- identificare soluzioni tecnologiche e organizzative
- valutare l'efficacia delle azioni intraprese



3 Cyber Incident response experience

Simulazione incidente per:

- sviluppare capacità decisionali sotto pressione
- elaborare protocolli di risposta



4 Re-check situazione aziendale

A distanza di 6/8 mesi vengono verificate con l'impresa le raccomandazioni implementate al fine di suggerire possibili sviluppi del percorso

Percorso di crescita delle competenze - AVANZATA



GDPR

- Principi chiave Gdpr
- Diritti degli interessati
- Obblighi aziendali
- Misure tecniche e organizzative per la protezione dei dati e la gestione dei Data Breach



ISO/IEC 27001

- Processi in ottica di risposta agli incidenti
- Gestione continuità operative
- Panoramica normative cybersecurity nazionali e internazionali (NIS II, ISO/IEC 27001)



NIS 2

- Identità digitali e accessi
- Processi di autenticazione e autorizzazione
- Perimetro sicurezza e superfici di attacco
- Sicurezza di rete

Casi studio di incidenti cyber



ANALISI

Attraverso la presentazione di **Business case reali** in ambito Information e Cybersecurity, si definiscono

- il contesto e
- le problematiche

incontrate nella gestione di incidenti informatici o minacce alla sicurezza delle informazioni.



IDENTIFICAZIONE

Si studiano le **soluzioni tecnologiche e organizzative** implementate dalle realtà colpite da incidenti e attacchi informatici, al fine di comprendere le strategie di sicurezza informatica messe in atto dalle stesse in ottica di gestione e mitigazione dei danni conseguenti.



VALUTAZIONE

Successivamente all'identificazione delle strategie di sicurezza adottate nella gestione di incidenti e attacchi informatici, viene fornita una **valutazione dell'efficacia** dell'implementazione delle stesse, al fine di estrapolarne errori e conseguenti lezioni apprese.

Cyber incident response experience (CIRE)



SIMULAZIONE OPERATIVA

Tramite un approccio originale all'**apprendimento operativo ed esperienziale**, l'azienda partecipa ad un **laboratorio di simulazione**: si affrontano scenari di risposta agli incidenti cyber in tempo reale, al fine di sviluppare capacità decisionali sotto pressione attraverso l'esperienza diretta in ambiente simulato.



DYNAMIC RULE SHIFTING

Tramite una metodologia di "**position rotation**" ogni partecipante sperimenta prospettive operative diverse dalla propria: utilizzando un approccio che si rifà alla "**Cross-Functional Immersion**", i partecipanti vivono le dinamiche dell'incidente da diverse prospettive operative, replicando le complessità di un'infrastruttura aziendale interconnessa.



GESTIONE INCIDENTE

Simulazione immersiva e interattiva che cala i partecipanti nella gestione di uno scenario di incidente informatico in tempo reale. Questo approccio punta ad accelerare i tempi di risposta e sviluppare un approccio proattivo alla sicurezza, al fine di generare best practice basate sull'esperienza operativa.



Re-check situazione aziendale

Il re-check della situazione aziendale punta a fornire una **fotografia del livello di maturità cyber** dopo che l'impresa ha svolto il percorso Information & Cybersecurity Base.

Con l'attività proposta l'azienda, grazie alle raccomandazioni fornite al termine dell'analisi iniziale (percorso Base):

1

verifica l'esposizione a minacce e rischi

2

migliora la propria postura cyber

Offerta avanzata

	PICCOLA IMPRESA	MEDIA IMPRESA	GRANDE IMPRESA
Valore della proposta	4.950 € + IVA	6.325 € + IVA	9.900 € + IVA
Finanziamento	80%	70%	40%
Quota a carico	990 € + IVA*	1.897,50 € + IVA*	5.940 € + IVA*

Offerta base + avanzata

	PICCOLA IMPRESA	MEDIA IMPRESA	GRANDE IMPRESA
Valore della proposta	9.350 € + IVA	11.825 € + IVA	18.700 € + IVA
Finanziamento	80%	70%	40%
Quota a carico	1.870 € + IVA*	3.547,50 € + IVA*	11.220 € + IVA*

IL TEAM



Cristina Colucci

Responsabile Area Compliance,
DPO e Consulente privacy
certificato



Nicola D'Angelo

Compliance &
Cybersecurity Consultant



Sonia De Marchi

Responsabile BU Servizi di
Trasformazione Digitale



Federica Lombardi

Compliance &
Cybersecurity Consultant



Luca Mancino

Innovation Consultant



Marco Ramella Votta

Responsabile Business Development & Sales

GRAZIE

PER LA TUA ATTENZIONE

Contattaci: Marco Ramella Votta

 [+39 3346240282](tel:+393346240282)

 www.piemonteinnova.it

 marco.ramella@piemonteinnova.it

 Via Vela 3, Torino

