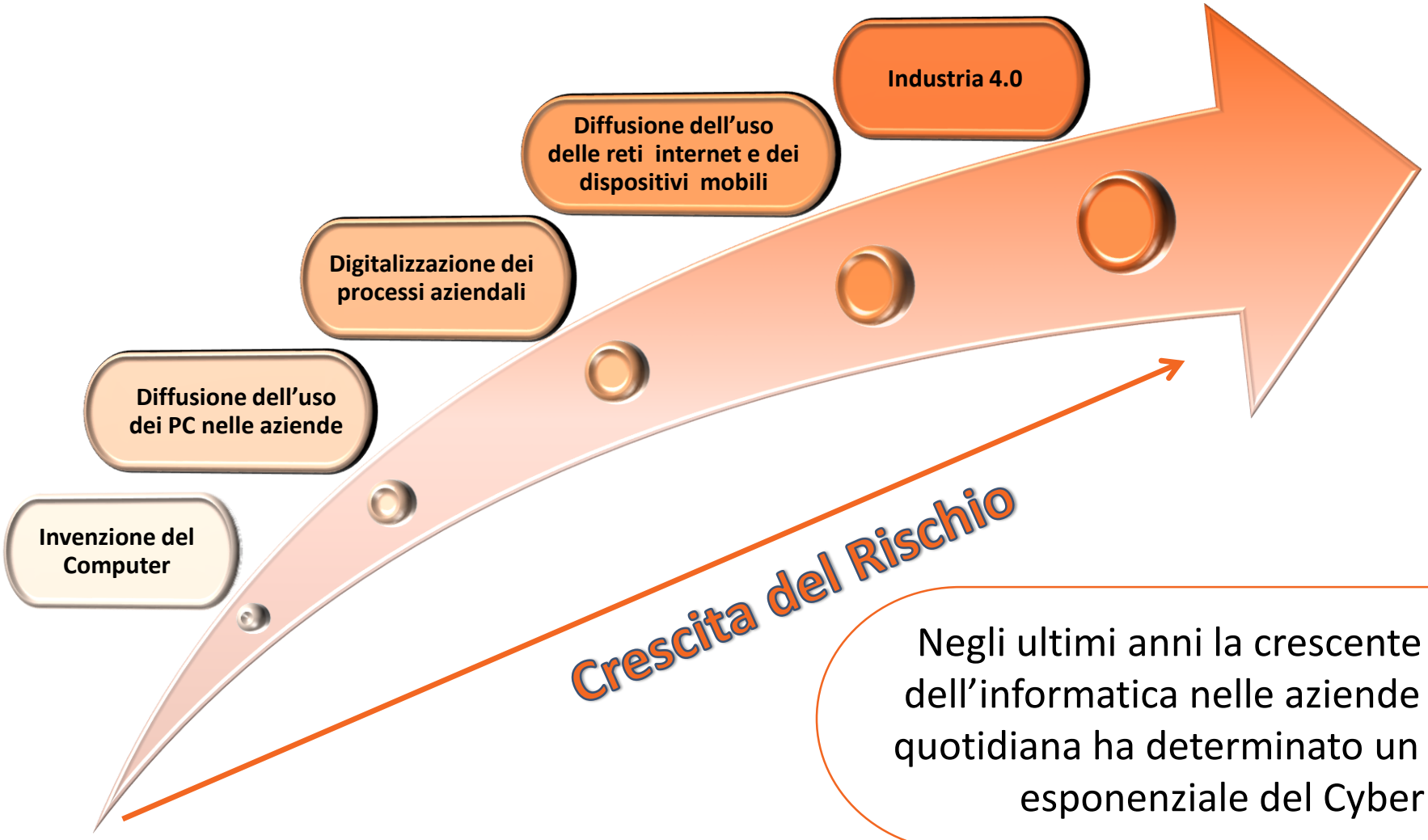
Cyber Risk

CYBER RISK O RISCHIO INFORMATICO

È il rischio di subire perdite economico/ finanziarie o danni reputazionali in conseguenza del verificarsi di eventi accidentali o di azioni dolose inerenti il sistema informatico (hardware, software, banche dati, etc.).

CRESCITA DEL RISCHIO INFORMATICO



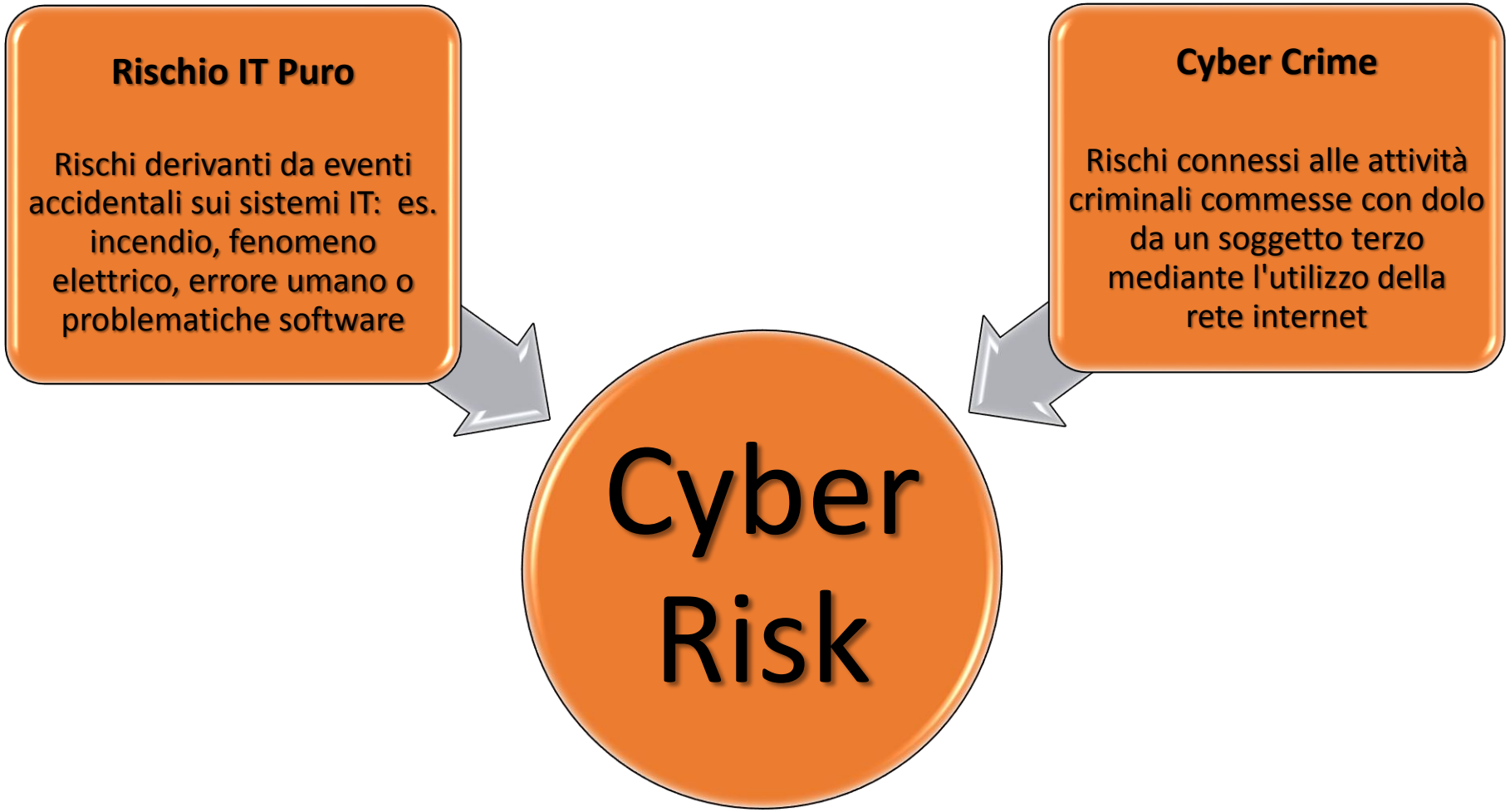
Negli ultimi anni la crescente diffusione dell'informatica nelle aziende e nella vita quotidiana ha determinato un incremento esponenziale del Cyber Risk

GRADUATORIA 2018 DEI RISCHI PIÙ TEMUTI DALLE IMPRESE ITALIANE

POSIZIONE	Rischio	%	Posizione precedente	Trend
1	Danni da interruzione di esercizio	51%	1 (36%)	=
2	**Attacchi cyber**	**38%**	**4 (23%)**	↑
3	Catastrofi naturali	30%	3 (25%)	=
4	Perdita della reputazione o del valore del brand	23%	10 (9%)	↑
5	Incendio, esplosioni	17%	6 (16%)	↑
6	Nuove tecnologie	16%	-	↑
7	Novità legislative e regolamentari	14%	7 (14%)	=
8	Sviluppi di mercato (volatilità, concorrenza, ecc.)	13%	2 (20%)	↓
9	Cambiamento climatico	11%	-	↑
10	Rischi ambientali (inquinamento)	10%	-	↑

Fonte: Allianz Risk Barometer 2018

FATTISPECIE DEL CYBER RISK



DANNI PIÙ COMUNI DA INCIDENTI CYBER

LE DIMENSIONI DEL FENOMENO: MONDO

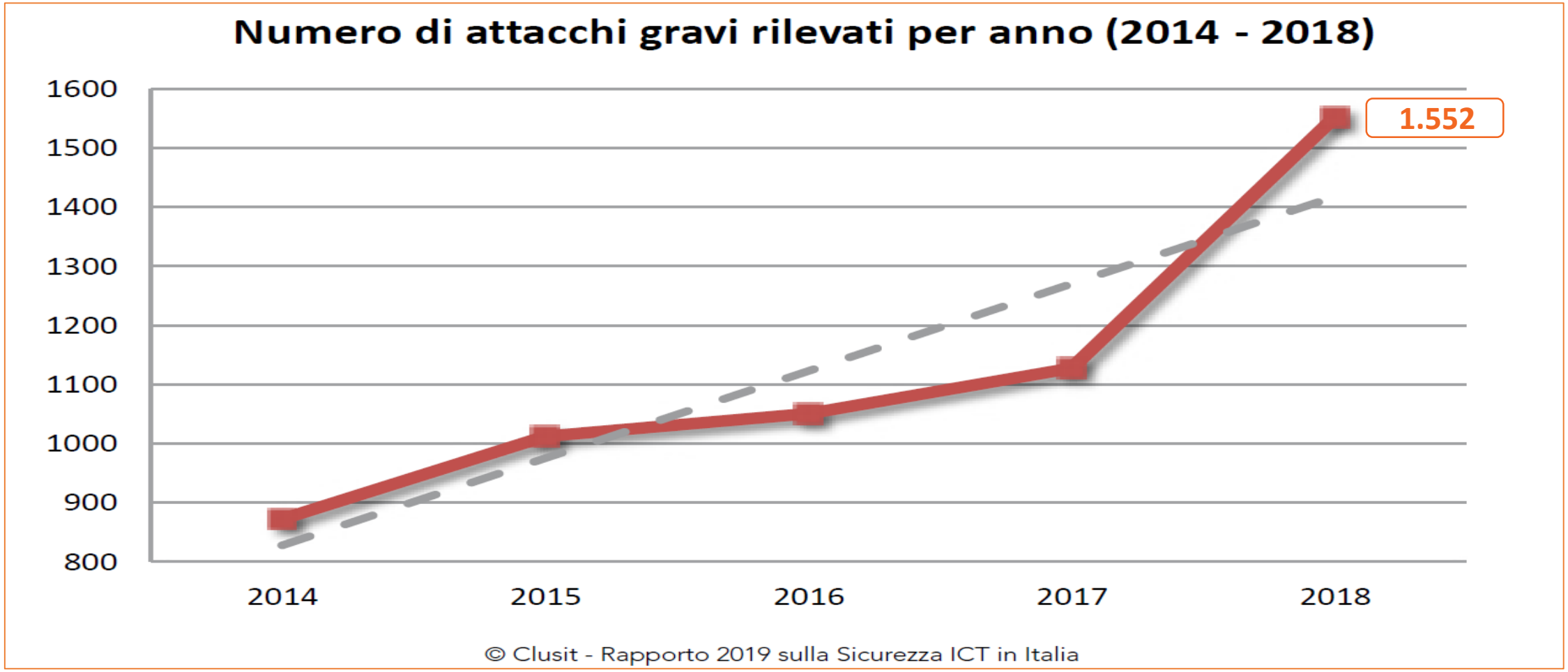
500 miliardi di dollari sono i danni causati dal cyber-crime nel 2017 a livello globale secondo il Rapporto 2018 della CLUSIT – Associazione Italiana per la Sicurezza Informatica.

180 miliardi di dollari è la perdita stimata nel 2017 è per i soli cittadini a livello mondiale secondo il rapporto CLUSIT 2018

11,7 milioni di dollari è il danno medio per le maggiori aziende nel mondo per eventi da cybercrime secondo il report «Cost of Crime Study» realizzato da Accenture e Ponemon Istitute

Il 60% delle aziende americane possiede una polizza contro i Cyber Risk secondo il network internazionale di consulenza BDO International Limited

ANDAMENTO GLOBALE DEGLI ATTACCHI GRAVI



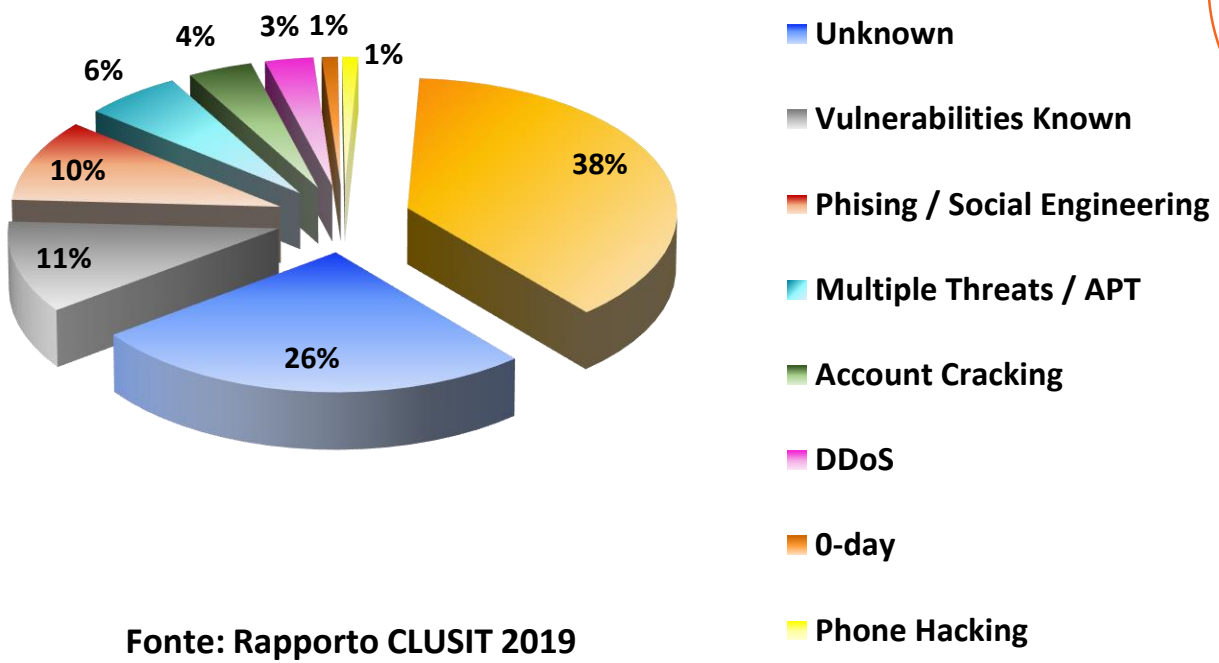
ANDAMENTO GLOBALE DEGLI ATTACCHI GRAVI PER TIPOLOGIA

Attacchi per tipologia	2014	2015	2016	2017	2018	2018 su 2017	Trend
Cybercrime	526	684	751	857	1232	43,8%	
Hacktivism	236	209	161	79	61	-22,8%	
Espionage/ Sabotage	69	96	88	129	203	57,4%	
Cyber Warfare	42	23	50	62	56	-9,7	
TOTALE	**873**	**1.102**	**1.050**	**1.127**	**1.552**	**37,7%**	

Fonte: Rapporto CLUSIT 2019

DISTRIBUZIONE DEGLI ATTACCHI GRAVI PER TECNICA D'ATTACCO

Tipologie e distribuzione delle tecniche d'attacco 2018

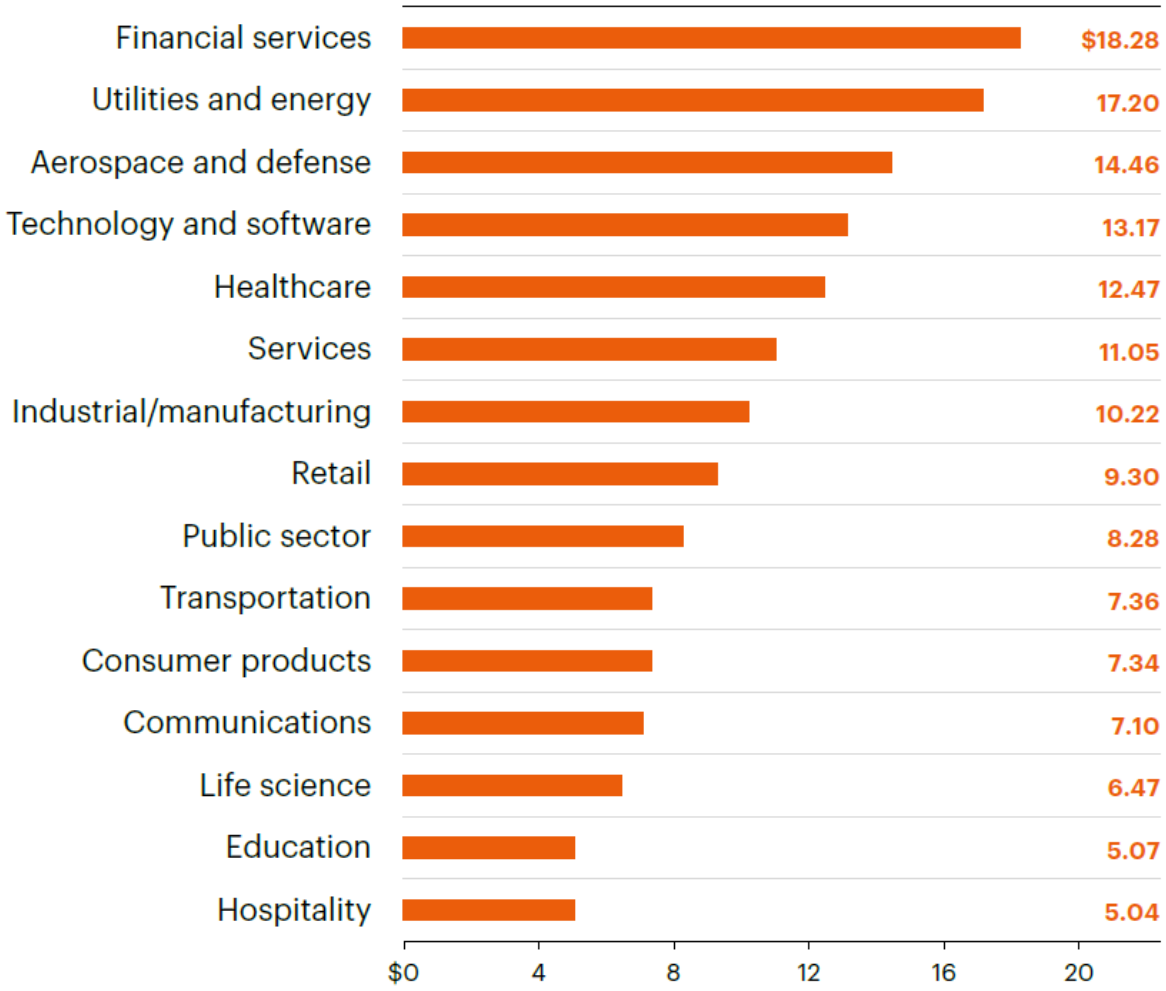


Fonte: Rapporto CLUSIT 2019

Il 62% degli attacchi più gravi registrati nel 2018 contro primarie organizzazioni è stato effettuato con le tecniche d'attacco più banali (SQLi, DDoS, Vulnerabilità note, Phishing e Malware)

Gli attacchi anche i più gravi vengono realizzati con relativa semplicità, a costi molto bassi e in via di ulteriore riduzione

COSTO MEDIO ANNUO PER SETTORE DI ATTIVITÀ (MONDO)



LE DIMENSIONI DEL FENOMENO: ITALIA

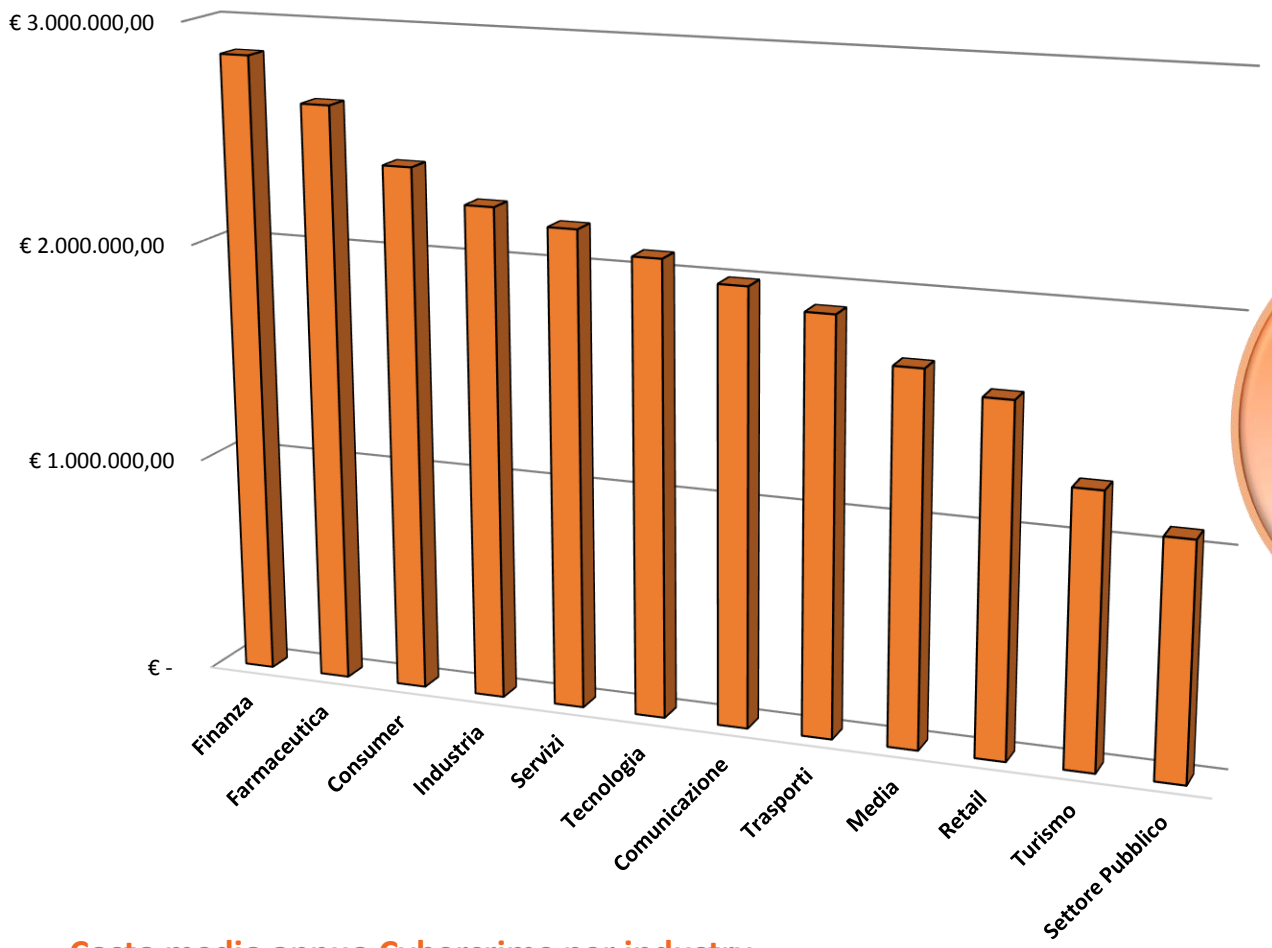
10 miliardi di euro sono i danni causati dal cyber-crime nel 2017 in Italia secondo il Rapporto CLUSIT 2018 e il rapporto Eurispes 2017

35 mila euro è il danno medio per le PMI in Italia nel 2017, anno in cui oltre il **50% delle PMI ha subito** un attacco cyber (Fonte: AIBA e Kaspersky Lab)

Oltre il 50% delle PMI ha subito almeno un attacco cyber nel 2017 (Fonte: AIBA)

Multe fino al 4% del fatturato o 20 milioni di euro per le aziende che non comunichino tempestivamente un'avvenuta fuga di dati in base al regolamento GDPR entrato in vigore nel 2018

LE DIMENSIONI DEL FENOMENO: ITALIA



Costo medio annuo Cybercrime per industry

2 milioni di euro è il costo medio degli incidenti cyber per le grandi aziende italiane
I settori più colpiti sono la Finanza e l'Industria Farmaceutica
(Fonte: HPE su dati Ponemon Istitute)

INVESTIMENTI IN SICUREZZA IT IN ITALIA NEL 2018

1.190 milioni di euro

è il totale degli investimenti in sicurezza IT in Italia nel 2018

in crescita del 7% rispetto al 2017 (Fonte: Osservatorio del Politecnico di Milano)

75% degli investimenti in sicurezza IT ha riguardato le grandi imprese	• Il **63%** delle grandi imprese ha aumentato il budget dedicato • il **30%** lo ha mantenuto stabile • Il **7%** ha diminuito il budget
25% circa delle aziende italiane è ancora indietro sulla sicurezza IT	• Il 13% non prevede un piano d'investimenti specifico • Il 6% investirà solo in caso di necessità • Prevalentemente sono le piccole imprese che investono poco in sicurezza IT
5 mila euro circa è l'investimento medio in sicurezza IT delle PMI	• Si va dai 3.180 euro di una piccola impresa manifatturiera • Ai 19.080 euro di una piccola impresa del settore ICT • Fino ai 44.590 euro delle grandi imprese (Fonte: Banca d'Italia)

CYBER RISK E ASSICURAZIONI

Il Cyber Risk è un rischio trasversale che risulta correlato con tutti i settori aziendali, da quello produttivo a quello finanziario, perché i sistemi IT sono indispensabili per tutte le aziende

Le piccole imprese sono più esposte al rischio in quanto in genere gestiscono il rischio in maniera approssimativa e con budget limitati in sicurezza IT

Il tessuto imprenditoriale italiano, basato sulle PMI risulta vulnerabile e particolarmente esposto a tale rischio, tuttavia gli investimenti in sicurezza IT sono in forte crescita

Prevenzione e Protezione sono necessarie ma non sufficienti:
PREVENIRE TOTALMENTE UN ATTACCO CYBER NON E' POSSIBILE

LA COPERTURA ASSICURATIVA CONSENTE DI TRASFERIRE LA COMPONENTE DI RISCHIO RESIDUO INELIMINABILE

LE DIMENSIONI DEL MERCATO «CYBER INSURANCE»

La valore del mercato della *Cyber Insurance* a livello globale è di **4 miliardi di dollari**. Gli USA sono il primo mercato mondiale e l'Europa è il secondo

Nel 2020 il valore del mercato globale raggiungerà i **7,5 miliardi di dollari** raddoppiando i valori attuali (Fonte: Insurance Information Institute)

In Italia il mercato delle assicurazioni Cyber vale circa **20 milioni di euro** al 2017 (Fonte: AIBA)

Solo il **15%** delle imprese italiane ha attivato coperture assicurative Cyber e circa la metà ha sottoscritto polizze dedicate e non generaliste

Le previsioni indicano che il mercato seguirà un **trend di crescita esponenziale anche in Italia** stimolato dal GDPR e dalla diffusione dei cyber attacchi

Il Mercato Cyber Insurance italiano

Il mercato assicurativo Cyber italiano ha ancora le caratteristiche del mercato poco sviluppato:

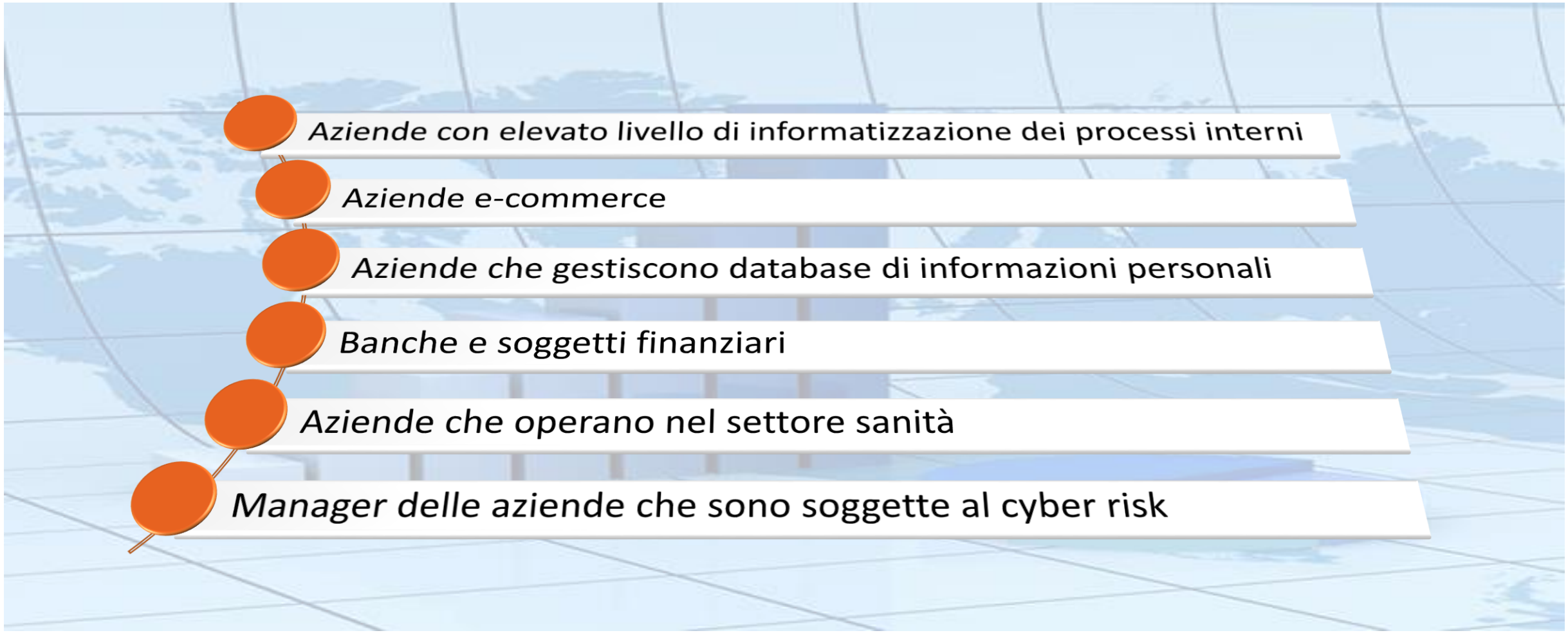
Dal lato della Domanda:

- **Carenza adeguata cultura sulla sicurezza cyber**
- **Manca la piena consapevolezza del rischio**
- **Costi delle polizze sono percepiti come troppo alti**
- **Alta probabilità di accadimento**

Dal lato dell'Offerta:

- **Mancanza modelli standard di riferimento**
- **Carenza dati statistici sufficiente**
- **Difficoltà stima dei danni**
- **Bassa competenza degli intermediari**

IL TARGET DEL CYBER INSURANCE ITALIANO



Il Mercato Cyber Insurance italiano

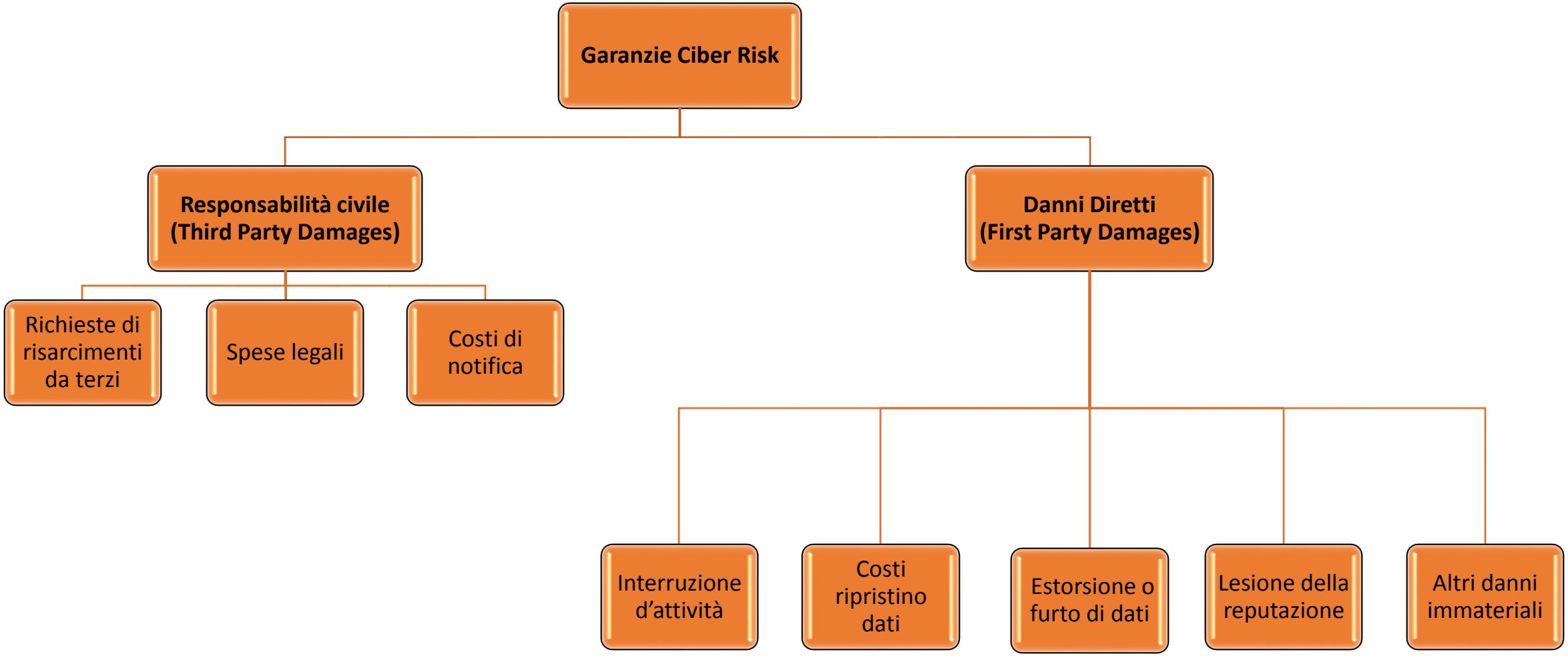
I testi delle polizze tradizionali risultano inadeguate ad affrontare il rischio cyber o lo escludono esplicitamente.

Tutti i maggiori Assicuratori italiani hanno predisposto o stanno strutturando dei prodotti specifici per il Cyber Risk.

Le coperture Cyber può presentarsi:
1) come garanzia aggiuntiva (Add-on) ad altre polizze tradizionali;
2) come contratti specifici (Stand-alone)

Oggi si osservano ancora forti disparità: anche le polizze Cyber possono essere limitate nel tipo di copertura, escludendo ad es. il rischio IT puro.

LE PRINCIPALI GARANZIE DELLE POLIZZE CYBER



I NOSTRI SERVIZI

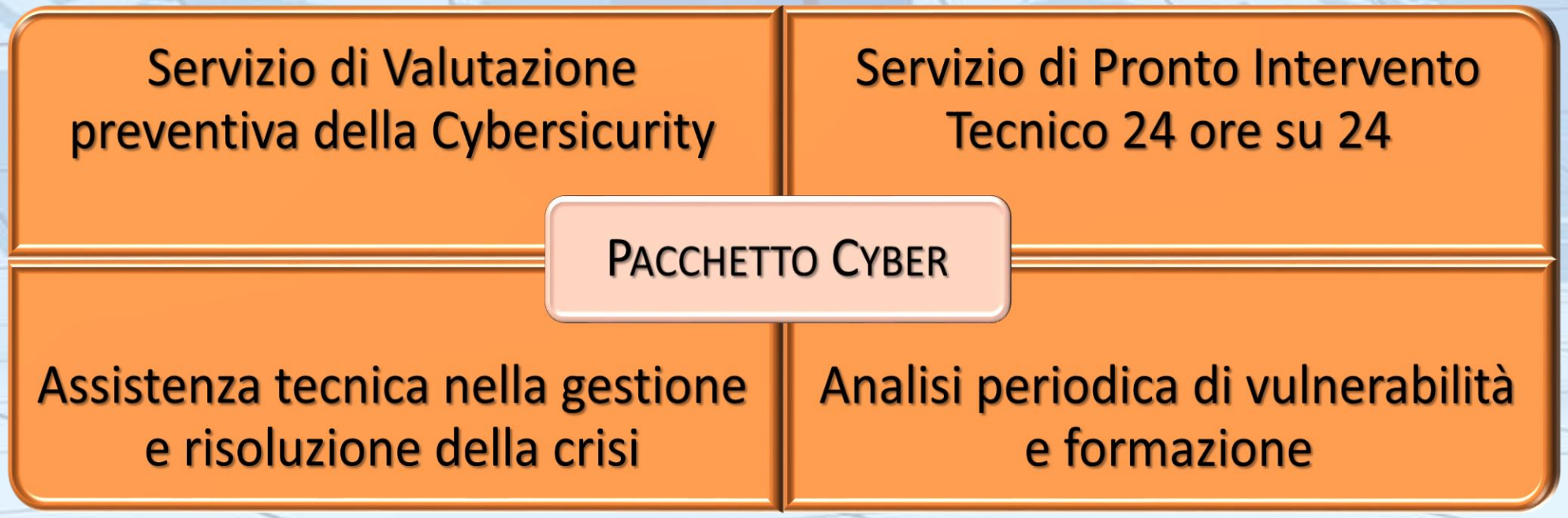
Un aspetto importante che fa la vera differenza nell'attuale sistema di offerta è quello dei servizi collegati alla copertura Cyber

La presenza di servizi a valore aggiunto rendono il prodotto assicurativo un pacchetto completo e innovativo per la gestione del rischio sia in termini di prevenzione ex ante che di gestione della crisi ex post.

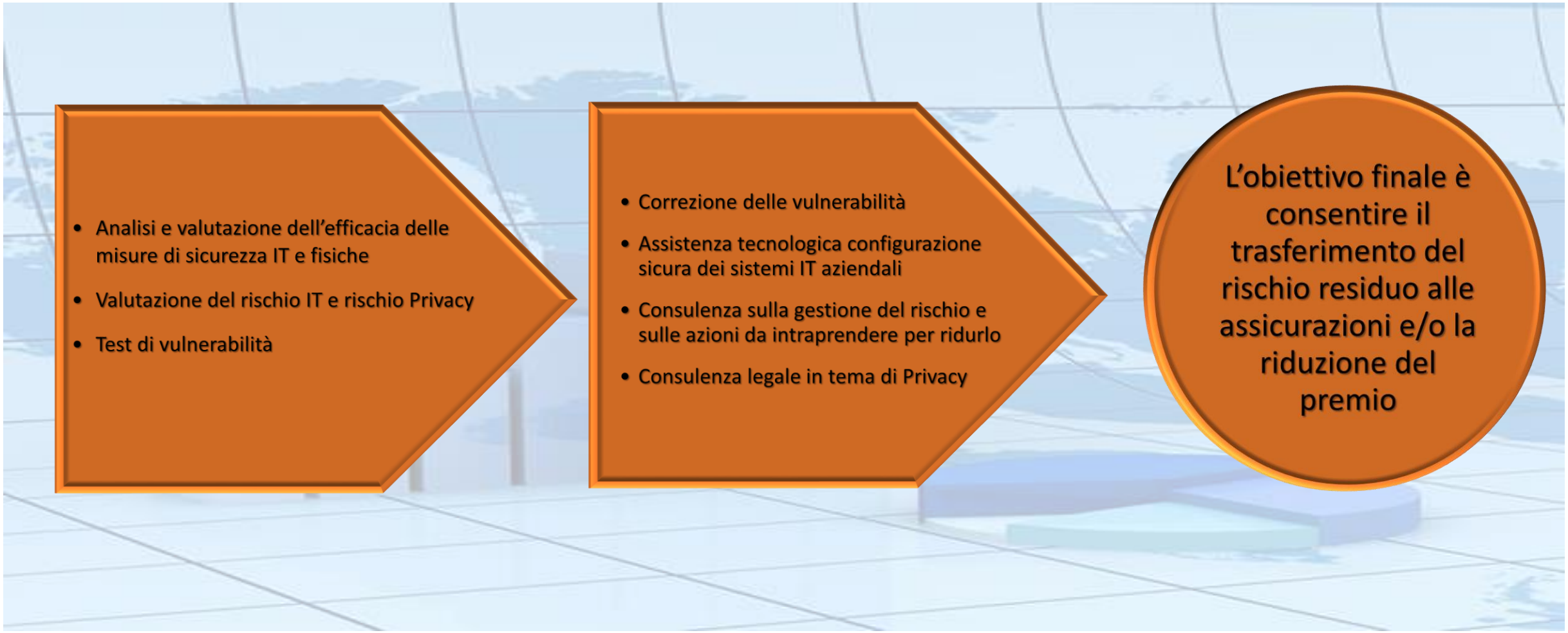
STARGEST grazie alla partnership con SIRTI è in grado di affiancare all'attività propriamente peritale una serie di servizi innovativi ad alto valore aggiunto

I NOSTRI SERVIZI

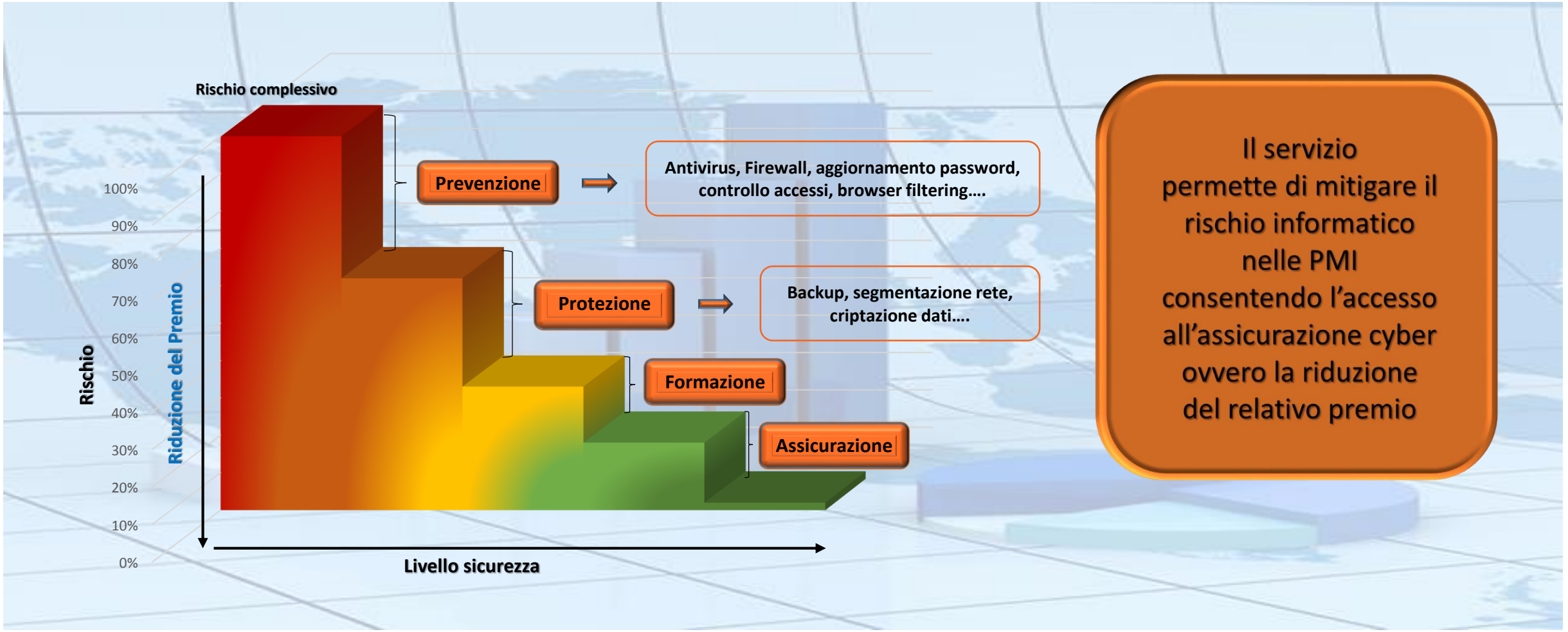
STARGEST in collaborazione con l'azienda partner **SIRTI** ha sviluppato un pacchetto di servizi innovativi per la gestione del rischio informatico nell'ambito della diversificazione dei servizi non solo peritali



SERVIZIO DI VALUTAZIONE PREVENTIVA DI SICUREZZA (EX-ANTE)

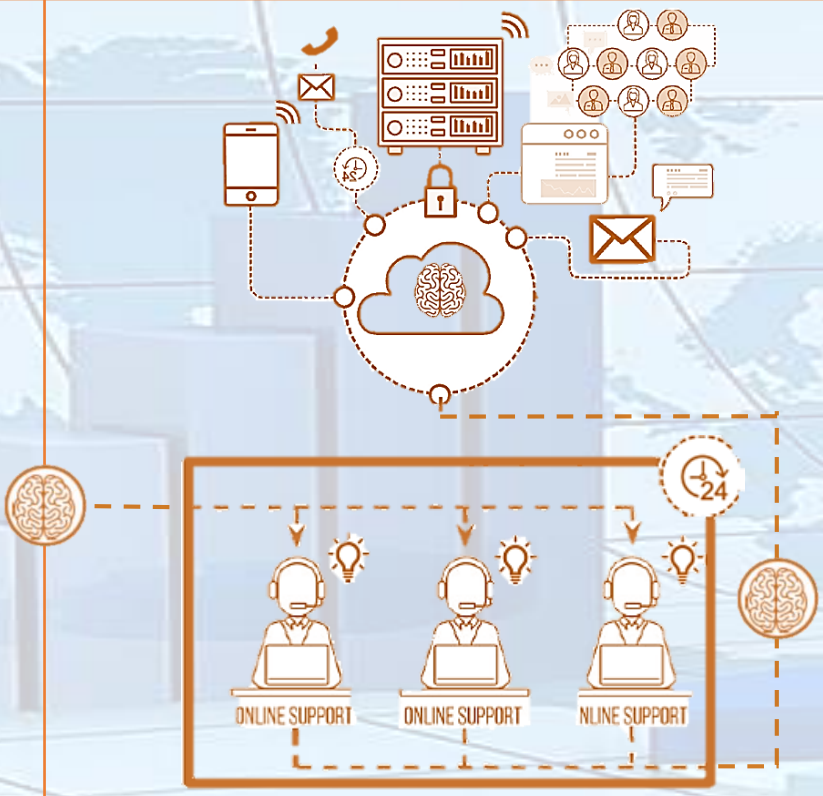


SERVIZIO DI VALUTAZIONE PRELIMINARE E ASSICURAZIONE

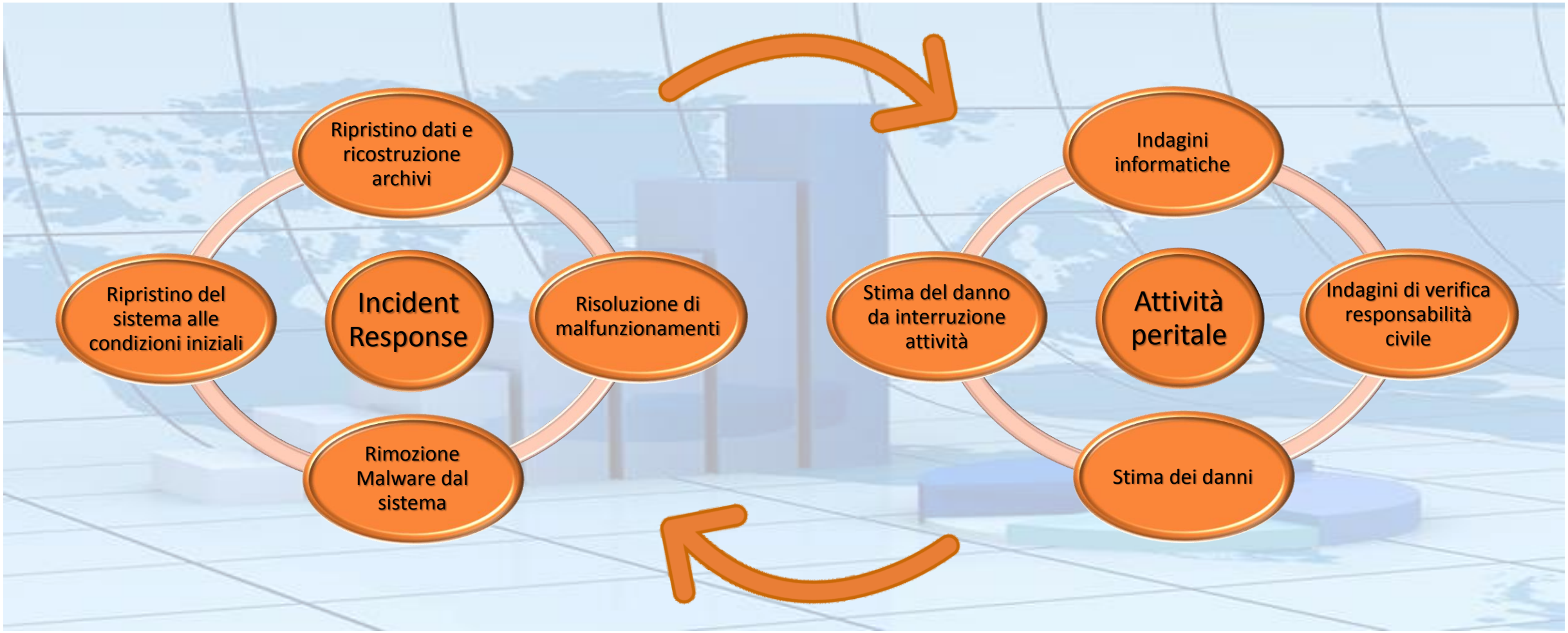


Il servizio permette di mitigare il rischio informatico nelle PMI consentendo l'accesso all'assicurazione cyber ovvero la riduzione del relativo premio

SERVIZIO DI PRONTO INTERVENTO

PIATTAFORMA DIGITALE	PRONTO INTERVENTO CENTRALE H24	INTERVENTO TECNICO SUL CAMPO
PROCESSI SISTEMI DI SUPPORTO INFORMAZIONI CONOSCENZA CONDIVISA		
La piattaforma Digitale dà supporto operativo e rende disponibili informazioni, sistemi e processi	Il Centro di Assistenza è composto da esperti che danno supporto 24 ore su 24 da remoto	Il servizio centrale condivide dati e video con i tecnici sul campo per gli interventi più complessi

SERVIZIO DI ASSISTENZA TECNICA (EX-POST)



INTERVENTO DIRETTO SUL CAMPO

SIRTI

Un tecnico della Sirti si recherà presso l'assicurato con un perito della Stargest e si occuperà di:

- Risolvere i malfunzionamenti
- Ripristinare i sistemi
- Effettuare un'indagine informatica sulle cause dell'evento
- Valutare il danno informatico

STARGEST

Un perito della Stargest si recherà presso l'assicurato con un tecnico della Sirti e si occuperà di:

- Verificare la polizza e la copertura del rischio
- Verificare la documentazione collegata al sinistro
- Effettuare la stima dei danni
- Effettuare l'attività peritale

ANALISI PERIODICA DI VULNERABILITÀ E ATTIVITÀ FORMATIVA