

**// howden | ASSITECA**



**CONFINDUSTRIA VICENZA**

# **CYBER RISK & SECURITY**

Come proteggere e assicurare  
la mia azienda



# SECURITY

**13 aprile 2023**

**Alessio Dichio  
Emanuele Capra**

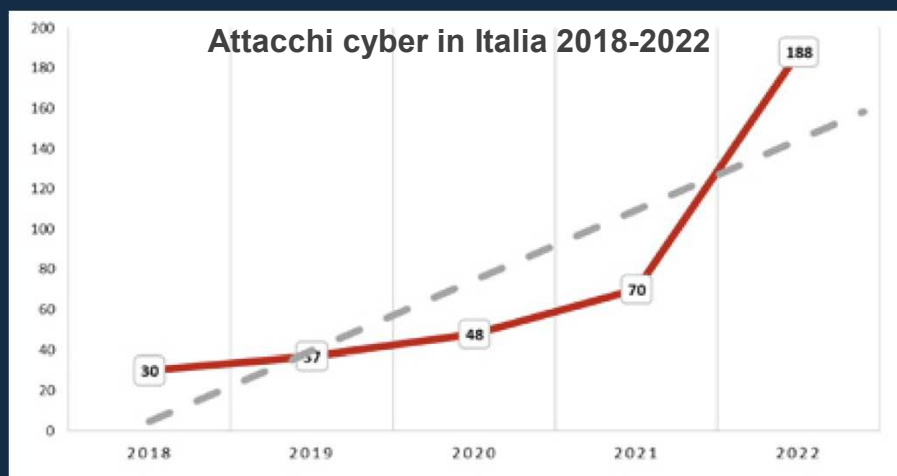
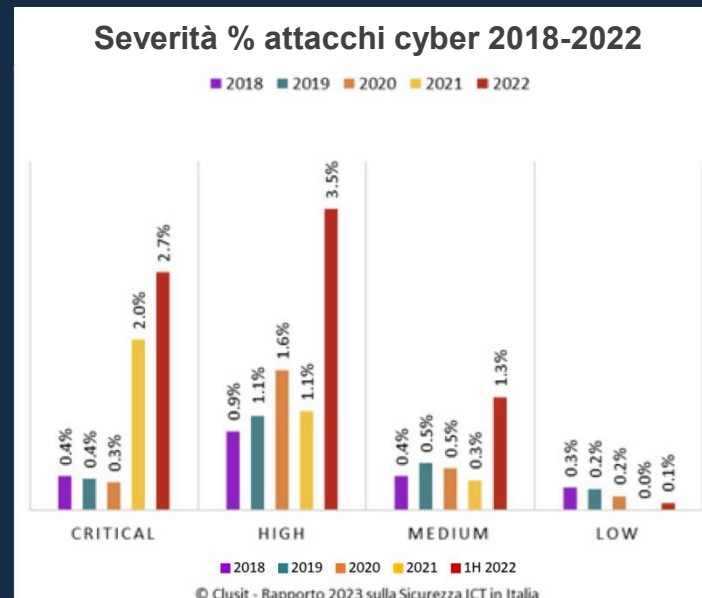


# AZIENDE ITALIANE SOTTO ATTACCO

## I trend

**Top 10 risks in Italy**  
 Source: Allianz Global Corporate & Specialty  
 Figures represent how often a risk was selected as a percentage of all responses for that country  
 Respondents: 38. Figures don't add up to 100% as up to three risks could be selected

Rank		Percent	2022 rank	Trend
1	Cyber incidents (e.g. cyber crime, malware/ransomware causing system downtime, data breaches, fines and penalties)	47%	1 (52%)	→
2	Business interruption (incl. supply chain disruption)	37%	2 (45%)	→
3	Energy crisis (e.g. supply shortage/outage, price fluctuations)	32%	NEW	↑
4	Macroeconomic developments (e.g. inflation, deflation, monetary policies, austerity programs)	21%	10 (10%)	↑
5	Climate change (e.g. physical, operational and financial risks as a result of global warming)	18%	8 (13%)	↑
6	Changes in legislation and regulation (e.g. trade wars and tariffs, economic sanctions, protectionism, Euro-zone disintegration)	16%	4 (23%)	↓
7	Natural catastrophes (e.g. storm, flood, earthquake, wildfire, extreme weather events)	13%	3 (33%)	↓
8	Fire, explosion	11%	NEW	↑
8	Market developments (e.g. intensified competition/new entrants, M&A, market stagnation, market fluctuation)	11%	5 (16%)	↓
8	Political risks and violence (e.g. political instability, war, terrorism, civil commotion, strikes, riots, looting)	11%	NEW	↑



**Attacchi rilevati dalla Polizia Postale 2021-22**

Attacchi infrastrutture critiche ad istituzioni, aziende e privati	2021	2022*	Variazione percentuale
Attacchi rilevati	5.434	12.947	+138%
Persone indagate	187	332	+78%
Alert diramati	110.524	113.226	+2%
Richieste di cooperazione HTC	60	77	+28%

\* - dati rilevati il 27/12/2022

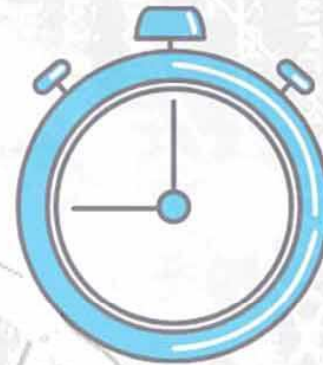
23: Distribuzione dei cyber attacchi in Italia nel periodo 2018-2022

# AZIENDE ITALIANE SOTTO ATTACCO

I trend

## Global Ransomware Damage Costs\*

- **2015: \$325 Million**
- **2017: \$5 Billion**
- **2021: \$20 Billion**
- **2024: \$42 Billion**
- **2026: \$71.5 Billion**
- **2028: \$157 Billion**
- **2031: \$265 Billion**



*Ransomware is expected to attack a business, consumer, or device every 2 seconds by 2031, up from every 11 seconds in 2021.*



\* SOURCE: CYBERSECURITY VENTURES

# AZIENDE ITALIANE SOTTO ATTACCO

## I dati delle assicurazioni

### Gli attacchi si intensificano

Il **48%** delle aziende ha riferito di aver subito un attacco informatico negli ultimi 12 mesi, rispetto al 43% dello scorso anno.

### Elevata percezione del rischio

Sette paesi su otto classificano un attacco informatico come la minaccia numero uno per le loro aziende.

### Pressione sui profitti

Tra le aziende attaccate, una su cinque attaccata afferma che la sua solvibilità è stata minacciata, con un aumento del 24% rispetto allo scorso anno.

### Rischi del remote working

Il Covid ha accelerato il passaggio al cloud, aumentando significativamente il numero di attacchi tramite cloud server.

### La competenza paga

I costi medi degli attacchi, in % sui ricavi, sono due volte e mezzo più alti per le aziende con scarse competenze cyber.

### Più polizze cyber

Il numero delle polizze è cresciuto del 12% rispetto a due anni fa (ma in US/UK sono molto più diffusa che in EU).

### Il ransomware cresce

Il 19% degli intervistati ha riferito di aver subito un attacco ransomware, in aumento rispetto al 16%. Due terzi delle aziende hanno pagato.

### Aumento delle spese

La spesa media per la sicurezza informatica delle aziende intervistate è aumentata del 60% nell'ultimo anno (+ 250% sul 2019).

### Impatto più grave

Il costo medio di un attacco è aumentato del 29% a poco meno di 17.000 dollari.

Paesi e aziende analizzate: Belgio (400), Francia (900), Germania (900), Irlanda (200), Paesi Bassi (400), Spagna (400), Regno Unito (900), Stati Uniti (900). Intervistati: 5.1818 responsabili cyber security

HISCOX  
Cyber Readiness  
Report 2022

# VENETO / VICENZA: AZIENDE SOTTO ATTACCO

## Gli ultimi incidenti

**IL GIORNALE DI VICENZA**  
/// CONFINDUSTRIA VICENZA

### Dalla Vecchia: «Gli attacchi informatici sono un allarme rosso per le imprese vicentine»

La presidente: «I danni di queste azioni sono enormi, in pericolo i dati, la privacy, i brevetti, se non la produzione»

07 febbraio 2023

Cybersicurezza: Confindustria Vicenza lancia l'allarme, l'attacco hacker di domenica scorsa è soltanto la punta dell'iceberg

**CRONACA**

### Attacco hacker Ulss 6 Euganea, pubblicati finora oltre 9.300 documenti: ci sono anche referti medici

Ora sul sito della cybergang LockBit 2.0 (dal nome del virus usato per entrare nel sistema informatico dell'azienda sanitaria locale) sono presenti migliaia di file sottratti all'Ulss 6 Euganea

16 gennaio 2022 09:02

**FEDAISF**

### Attacco hacker alla Zambon

26 Aprile 2021

**CRONACA VILLAFRANCA DI VERONA / CORSO GARIBOLDI**

### Publicati nel darkweb dati riservati copiati dal sito del Comune di Villafranca

A metà marzo, hacker avevano attaccato l'ente pubblico a scopo di ricatto. La somma richiesta non è stata pagata e così è circa 100 giga di informazioni anche di tipo personale sono state rese pubbliche

07 aprile 2022 11:06

**QUADRE**

### Piccole imprese e attacchi informatici: colpite 4 su 10. Le contromisure

16 Febbraio 2023

Le imprese venete sempre più soggette a reati informatici. Nell'ultimo anno, nella regione, sono cresciuti del 21,2%, un valore più alto rispetto alla media nazionale fermatasi ad un +18,4%. Settima regione in questa classifica in cui sveltano Toscana con +35,5%, Puglia con +25,0% e Lombardia con +24,8%.L'incidenza del fenomeno in Veneto è pari a 59 denunce ogni 10mila abitanti, anche in questo caso con una intensità superiore alla media italiana

**Vicenza. Attacco hacker alle Acciaierie Beltrame. L'azienda: «Stiamo verificando se sono stati compromessi dati»**

Martedì 14 Febbraio 2023 di Redazione Web

**VICENZA** - Il gruppo vicentino dell'acciaio **Beltrame** ha reso noto oggi di essere stato vittima di un **attacco informatico** lo scorso 11 febbraio, e di avere immediatamente attivato i protocolli di sicurezza. «Una task force dedicata, con il supporto di esperti di **cybersecurity** - si legge nella nota aziendale - ha intrapreso ogni azione volta a minimizzare l'impatto, identificare le cause e adottare le azioni risolutive. È in corso un'indagine per verificare se siano stati compromessi dati personali».

**San Donà. Attacco hacker alla casa di riposo, rubati anche i dati di 70 dipendenti. Interviene la polizia postale**

La Nuova di Venezia e Mestre, 20 gennaio 2022

**SAN DONA'**: Spuntano anche nomi e dati sensibili dei dipendenti della casa di riposo Monumento ai Caduti di San Donà. Non c'erano solo gli anziani ospiti della struttura nell'elenco pubblicato sul dark web dagli hacker che hanno preso di mira la società Isvo Srl che ha in gestione la casa di riposo di via San Francesco nel cuore della città.

**refe veneto**

### CORNEDO VICENTINO | ATTACCO HACKER AI SERVER DEL COMUNE, CRIPTATI TUTTI I DATI

08/02/2022 CORNEDO VICENTINO - Attacco hacker ai server del Comune di Cornedo Vicentino. I pirati informatici hanno criptato tutti i dati: il Sindaco ha attivato le Forze dell'Ordine, la Prefettura, la Procura e anche la Digos. || Attacco

# ITALIA: AZIENDE SOTTO ATTACCO

## Gli ultimi incidenti

ENTI PUBBLICI

Attacco hacker al sistema informatico del Comune di Sarno: serveri bloccati

Ottobre 2021

**LA STAMPA**

Ecco come l'Atc è finita sotto attacco: gli hacker hanno chiesto un riscatto da 700 mila dollari

Tutto in una notte: bloccati i server che gestiscono bollette e affitti. La situazione rischia di bloccare le attività

BERNARDO BASILICINI MENNE

12 Aprile, 2021

**COMUNICAZIONE IMPORTANTE**

Città di Maratea

Un attacco hacker ha bloccato le cartelle di rete e gli archivi digitali dell'Ente

Nei prossimi giorni il Comune di Maratea sarà sottoposto a un attacco ransomware

**EDIZIONE CASERTA**

Attacco hacker, bloccato il sistema dell'Arpac

Di redazione Caserta 19 Agosto 2022

Attualità, Caserta e Mariglianese

**LA STAMPA**

L'attacco hacker a Torino? I cittadini pagano l'incapacità dell'Asl di gestire i propri sistemi informatici

La colpa è dell'azienda che non ha investito nella cyber sicurezza e nella salvaguardia delle banche dati

UMBERTO RAPETTO\*

27 Agosto 2022 2 minuti di lettura

Aggiornato alle 11:39

Umberto Rapetto, generale della Guardia di Finanza già comandante del Gruppo Anticrimine Tecnologico

**LA STAMPA**

Il prezzo dell'attacco hacker? Alle casse del Comune di Rivoli è costato 50 mila euro

PATRIZIO ROMANO

19 Marzo 2022 alle 13:13 1 minuto di lettura

**Italia**

Attacco hacker alla Regione Sardegna, migliaia di file finiscono sul dark web

25 giugno 2022

Coltivare anche direzioni di Enti locali e Protezione civile. Divulgati dati anagrafici, dati sanitari, informazioni sullo stato patrimoniale e finanziario

**CORRIERE DELLA SERA BRESCIA**

Attacco hacker al Comune di Brescia: «I dati rubati sono già in rete. Così funziona il ricatto online»

di Massimiliano Del Barba

11 ottobre 2021, 11:41

**L'Arena**

Attacco hacker al Comune di Villafranca: pubblicati 100 giga di files riservati

97 aprile 2022

Il Comune di Guasila (Dott. Sirigu)

**CRONACA SARDEGNA**

Attacco hacker al Comune di Guasila: cancellati tutti i dati

Lunedì 24 Agosto 2020 alle 18:25

**Attacco hacker all'Agenzia delle Entrate: "Rubati 78 giga di dati: cinque giorni per il pagamento del riscatto, senno pubblichiamo tutto"**

25 luglio 2022

**Attacco hacker al server che gestisce le multe del comune di Cherasco**

Redazione Corriere 8 Novembre 2021

Ultimo aggiornamento 8 Novembre 2021

1 minuto per la lettura

**Attacco hacker alla Banca d'Italia, nel mirino conti e risparmi**

La notizia riportata da un quotidiano. A lanciare l'allarme in una chat interna un dipendente contattato al telefono dallo stesso hacker ai primi di marzo

SANITA'

Attacco hacker ai server dell'ospedale di Alessandria. Violata la sicurezza informatica (R. Bobbio)

Di redazione genova 31/12/2022

Attacco informatico all'Ospedale Macedonio Melloni di Milano. E' stato Vice Society

Di redazione RHC 21/06/2022

11:16 pm

**TCOM24**

Milano, hacker attaccano ospedali Fatebenefratelli-Sacco: bloccati pronto soccorso

02 MAGGIO 2022 19:31

Cybersecurity, sotto attacco 24% strutture sanitarie

Presentato il rapporto di Stato e Università Torino per il 14% delle strutture sanitarie che è penetrato come una peste

Ospedale André Mignot di Versailles "Interventi chirurgici rimandati". Sistemi spenti a causa di un attacco ransomware.

Redazione RHC 08/12/2022

5:32 pm

**Padova, attacco hacker alla sanità: turni, stipendi, referti, denunce. Ecco che cosa hanno pubblicato sul web**

di Gabriele Fusar Poli

**Attacco informatico ai servizi sanitari di Como e Varese**

Publicati i dati sensibili di ottocento disabili delle due province. I "pirati" del web hanno chiesto un riscatto

di Marco Marelli

**il mattino**

Attacco hacker alla casa di riposo di San Donà: pubblicati i dati sensibili degli anziani

18 maggio 2022

Nonni e cugini, medici curanti, terapie e farmaci: è la stessa mano che ha colpito all'Asl di Padova. Riscatto non pagato

Attacco alla Regione Lazio: il ransomware ha sfruttato la vulnerabilità della VPN

16 settembre 2022, 12:05



**Attacco all'ASL Napoli 3 Sud blocca i vaccini: perché la Sanità italiana è cyber-fragile**

Di Dario Fadda



ISTITUZIONI

**LA STAMPA**

Attacco hacker al sito della Siae, sottratti 60 gigabyte di dati: chiesto un riscatto di 3 milioni di euro in bitcoin

Rubati circa 28mila documenti scrivibili appartenenti a diversi artisti, alcuni già in vendita sul dark web. Associazione: «Non pagheremo»



**Messaggero**

Gli hacker attaccano i registri elettronici di tre scuole: «Salta la lezione»



Colpiti gli istituti di Salses e Brugnera Manzonica, Delta Valseno e Cuneido. La denuncia del sindacato: «La rete è vulnerabile»

Chiara Binetti

**la Repubblica**

Roma, attacco hacker a Tor Vergata: colpisce le ricerche sul Covid, si blocca anche la didattica a distanza



«Questi i dati di docenti e allievi, compromessi oltre 700 computer a disposizione del personale. Il rettore: "Avviare contromisure per circoscrivere il danno, ripristinare dati e ricerche e assicurare il proseguimento della didattica"»

**Svastiche e porno: attacco hacker durante webinar "Roma oltre il Covid"**

Paolo Ciani: "Qualcuno non ama che le idee circolino? Svastiche, porno, bestemmie. E' pochezza intellettiva, tecnica ed informatica. Fascismo 4.0 d'attacco"

**Il Messaggero**

Foto e video sexy sui profili social, attacco hacker all'Accademia di Belle Arti di Frosinone

**Attacco hacker all'Associazione bancaria: online dati sensibili**

Una banca italiana è stata attaccata da un gruppo di hacker che ha rubato dati sensibili di clienti e dipendenti

Una volta il sito della Associazione bancaria italiana ha subito un attacco hacker che ha rubato dati sensibili di clienti e dipendenti

**Bilancio Sampdoria, attacco hacker e addio soldi. Il caso**

di Redazione



La Sampdoria deve mettere un segno nero sul bilancio di 800mila euro a causa di un attacco hacker della Russia...

Una cifra importante, pari a circa 800.000 euro, questa la cifra sottratta alla Sampdoria per mano di un attacco hacker. Una cifra non da poco, per la quale i doriani sono subito corsi ai ripari.

**Rai News**

Colpito in particolare Collettiva.it

**Cgil, nuovo attacco hacker: chiusi tutti gli accessi ai siti**

Un attacco "molto strutturato, proveniente da diverse fonti". Al momento gli accessi sono stati parzialmente riattivati

# ITALIA: PMI SOTTO ATTACCO

## Le statistiche

**eritel**  
passione per TICIT

**CYBERSECURITY:  
AUMENTATI DEL 38%  
IN UN ANNO GLI  
ATTACCHI  
INFORMATICI ALLE PMI**



**B2BLABS**  
Startup 5G Trasformazione Digitale Intelligenza Artificiale Sicurezza Informatica

### Assiteca: "Cresciute del 300% le assicurazioni per cyberattacchi"

di **Antonino Caffo**  
Lunedì 26 luglio 2021 9:58  
3 min • val ai commenti

Più informazioni su  
Assiteca • cybersecurity • Cyber sicurezza • Scenario • Assiteca

Aumenta esponenzialmente il rischio di attacchi cyber. Da Microsoft a Kaseya, dalla Russia alla Cina, passando per gli USA, la globalizzazione della supply chain, che tocca in particolare le imprese con relazioni internazionali (in Italia l'83%), rende tutte le aziende soggette a rischio di incursioni digitali.

Si è appena assistito ad un attacco massiccio ransomware che partendo dalla Florida ha "infettato" molte aziende negli USA e da lì tante italiane, tra cui molte PMI dislocate in tutte le regioni. Ancora più eclatante il caso Microsoft, che apre a scenari da guerra fredda 2.0 fra USA e Cina.

**Adnkronos** GREEN PASS AFGHANISTAN

### Covid sveglia hacker, Pmi nel mirino

12 maggio 2021 | 16:40  
1.811 GUARDIA: 4 minuti

Cybersecurity, arriva il Dbir 2021 di Verizon Business. Larbey all'Adnkronos: "Si assottiglia gap fra grandi aziende e piccole imprese"

### Pmi italiane nel mirino delle cyber-gang: ora è record, ecco perché

di **Alessandro Longo**



*Lo dicono i dati 2022 appena usciti, del Clusit: l'aumento di attacchi cyber andati a segno, con danni economici, è aumentato del 168% in Italia, al top nel mondo*

18 MARZO 2023 ALLE 14:41 2 MINUTI DI LETTURA

Cybersecurity, in Italia c'è un attacco grave ogni 5 ore. Più 91,2% in 5 anni

**la Repubblica**

**PANORAMA**

CYBER SECURITY 22 Marzo 2023

### Cybersecurity: nel 2023 a rischio soprattutto le PMI

Redazione

**DiariodelWeb.it**

SICUREZZA INFORMATICA

### Un nuovo bersaglio: le piccole imprese vittime degli attacchi informatici

Nell'ultimo anno gli attacchi alle imprese sono aumentati del 13%, causando danni non indifferenti sia a livello di sicurezza informatica che a livello economico

REDAZIONE (BES)  
VENERDÌ 4 MARZO 2022 10:36

COSA FARE PER DIFENDERSI

### Ransomware, la nuova variante per attaccare Pmi, liberi professionisti e autonomi

di Redazione Key4biz  
12 Agosto 2021, ore 12:50

### Le dimensioni di un'azienda non contano quando si parla di sicurezza

Non sono solo le grandi aziende a doversi mettere al sicuro da possibili cyber attacchi. Anche le piccole e medie imprese sono diventate obiettivi "attraenti" per i criminali informatici, in un momento in cui il loro business online è aumentato considerevolmente e dovendo comunque dedicare tempo e talenti all'attività principale. Diversi report, riguardanti il primo semestre del 2020, hanno dato una panoramica delle PMI in relazione al grande tema della cybersecurity. Nello specifico, le indagini condotte mostrano come quasi l'84% delle PMI italiane abbiano rischiato un attacco informatico nel corso del 2020, anche a causa dell'emergenza Coronavirus.

# I RISCHI INFORMATICI

## La mappa

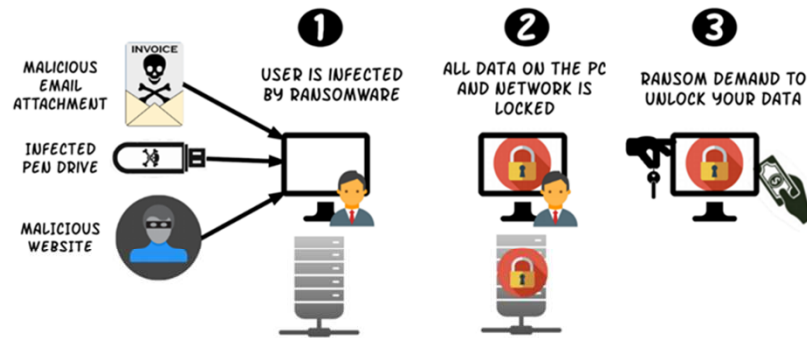




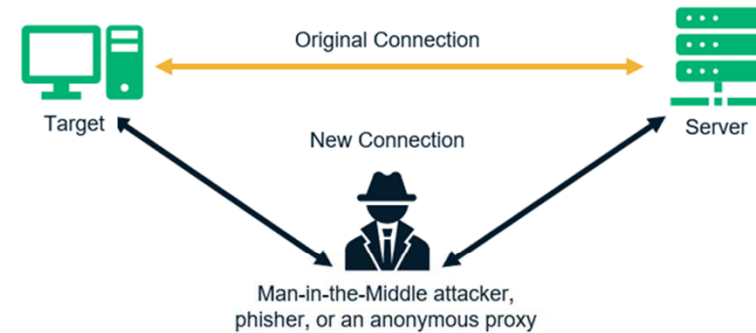
# ATTACCHI INFORMATICI

## I casi più frequenti rilevati da Assiteca - Howden

### RANSOMWARE



### TRUFFE



### DATA BREACH



### ATTACCHI MIRATI



# ATTACCHI INFORMATICI

## Eventi - Effetti - Danni - Attività

	Effetti		Danni		Cosa fare
Evento Cyber	Blocco dei sistemi informatici	Evitare che succeda di nuovo (azioni di miglioramento)	Costi di ripristino dei dati e/o dei sistemi	Ricostruzione della reputazione aziendale	Capire cosa sta succedendo
	Violazione di dati personali / sensibili		Spese extra (maggiori costi)		Non sbagliare gli interventi
	Danni a Terzi Social / Media		Perdita di profitto		Ripristinare i servizi rapidamente
	E-Crime		Costi di notifica		Definire se è un data breach
		Spese di Indagine	Costi di monitoraggio		Comunicare al Garante e gli Interessati
		Assistenza / difesa legale	Sanzioni		Intervenire per ridurre impatti
			Risarcimenti		Definire la responsabilità
			Perdita finanziaria		Proteggere la reputazione
					Definire la responsabilità
					Limitare i danni commerciali

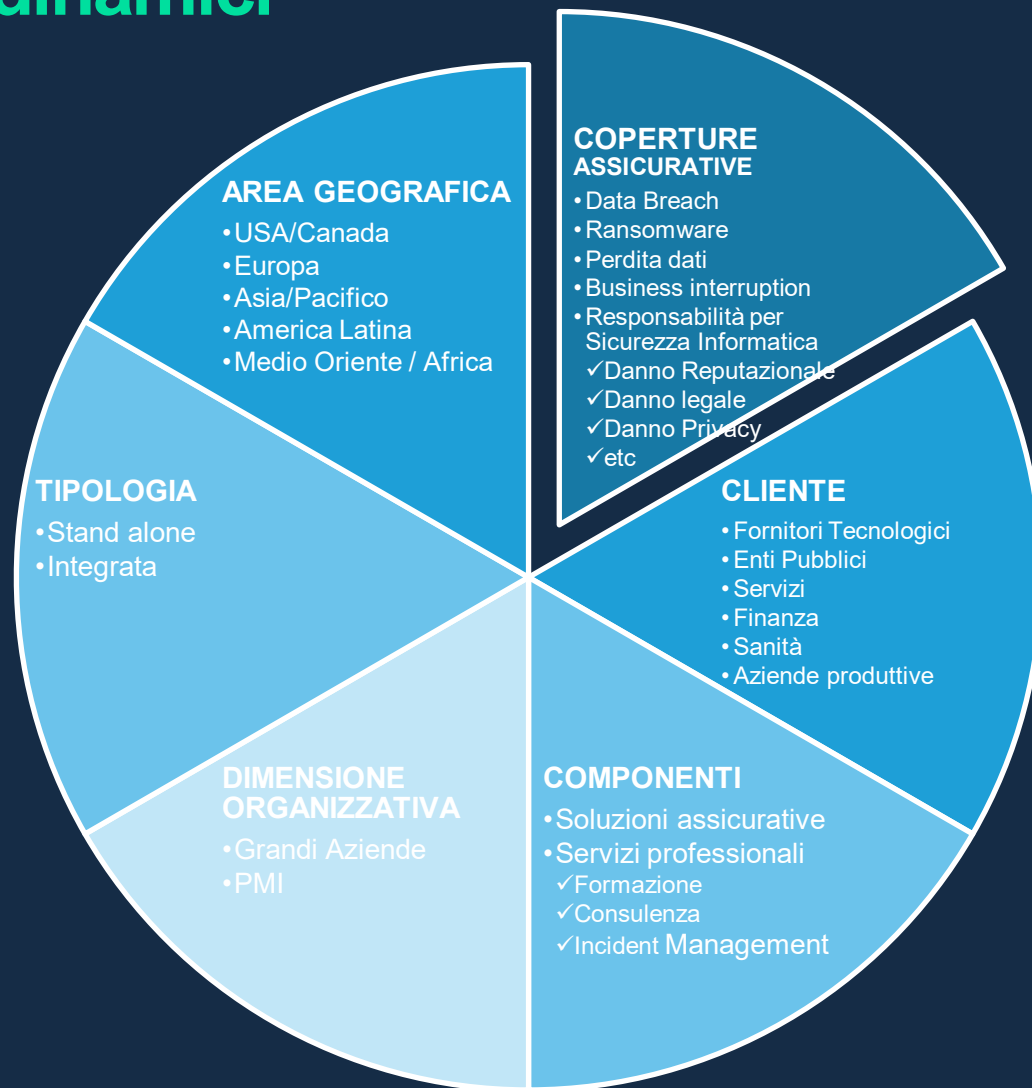
# GESTIONE EMERGENZE INFORMATICHE

## Incidente informatico: cosa succede e come gestire le prime 48 ore

INCIDENTE	ALERT	CRISIS RESPONSE	REMEDIATION/IMPROVEMENT	
	4-8 ore	48 ore	Da definire in base a complessità azienda e situazione	
	CHIAMATE O ALLARMI	ATTIVAZIONE CRISIS TEAM	ATTIVAZIONE REMEDIATION TEAM	
	<b>PRIMO CONTATTO</b> <ul style="list-style-type: none"><li>• Comprensione scenario</li><li>• Suggestimenti</li></ul>	<b>ANALISI SITUAZIONE</b> <ul style="list-style-type: none"><li>• Riunioni/call con IT azienda</li><li>• Analisi dati e LOG (triage)</li></ul> <b>DEFINIZIONE ATTIVITA'</b> <ul style="list-style-type: none"><li>• Contenimento – Eradicazione – Ripristino</li></ul> <b>INTERVENTI URGENTISSIMI</b>	<b>ATTIVITA' RIPRISTINO</b> <ul style="list-style-type: none"><li>• Contenimento, bonifica, messa in sicurezza, ripristino e/o monitoraggio.</li><li>• Gestione Data breach, truffe e/o altri crimini informatici;</li><li>• Assistenza legale, indagini forensi, perizie</li></ul>	<b>ATTIVITA' POST CRISI</b> <ul style="list-style-type: none"><li>• <i>Rimborsi assicurativi</i></li><li>• Marketing e Comunicazione</li><li>• Assessment (organizzativo e VA)</li><li>• Piano di miglioramento (tecnologie e procedure)</li><li>• Monitoraggi dati on line</li></ul>
	<b>OUTPUT</b> <ul style="list-style-type: none"><li>• Allertare Manager e IT Team</li></ul>	<b>OUTPUT</b> <ul style="list-style-type: none"><li>• Diario IT Manager</li><li>• Remediation Plan<ul style="list-style-type: none"><li>• Descrizione esiti, priorità ed approfondimenti,</li><li>• Attività necessarie, professionalità richieste e tempistiche suggerite</li></ul></li></ul>	<b>OUTPUT</b> <ul style="list-style-type: none"><li>• Progettazione e esecuzione Interventi di ripristino</li><li>• Rapporti stato avanzamento</li></ul>	<b>OUTPUT</b> <ul style="list-style-type: none"><li>• Rapporti indagini e danni</li><li>• Piano di miglioramento</li><li>• Implementazione tecnologie / procedure</li><li>• Rapporti monitoraggio on line</li></ul>

# IL MERCATO ASSICURATIVO CYBER

Una struttura sofisticata per rispondere a rischi complessi e dinamici



# IL MERCATO ASSICURATIVO

## La situazione 2023

### MERCATO SPECIALIZZATO

- **Numero limitato** di Compagnie Assicurative
- Assicuratori specializzati principalmente **stranieri**
- **Richieste informative sempre più ampie** sul rischio da assicurare.

### STATO DI HARD MARKET

- **Premi** assicurativi in costante aumento
- **Capacità** assuntive **in riduzione**
- **Maggiore selezione** dei rischi, contenimento delle esposizioni e sottoscrizione molto tecnica
- **Tempi** di quotazione **più lunghi**

### Mercato internazionale polizze cyber

*Il 43% è sottoscritto da 6 compagnie*



FitchRatings

Published May 2022

# IL MERCATO ASSICURATIVO CYBER

## Aumento significativo dei premi

In the line of fire

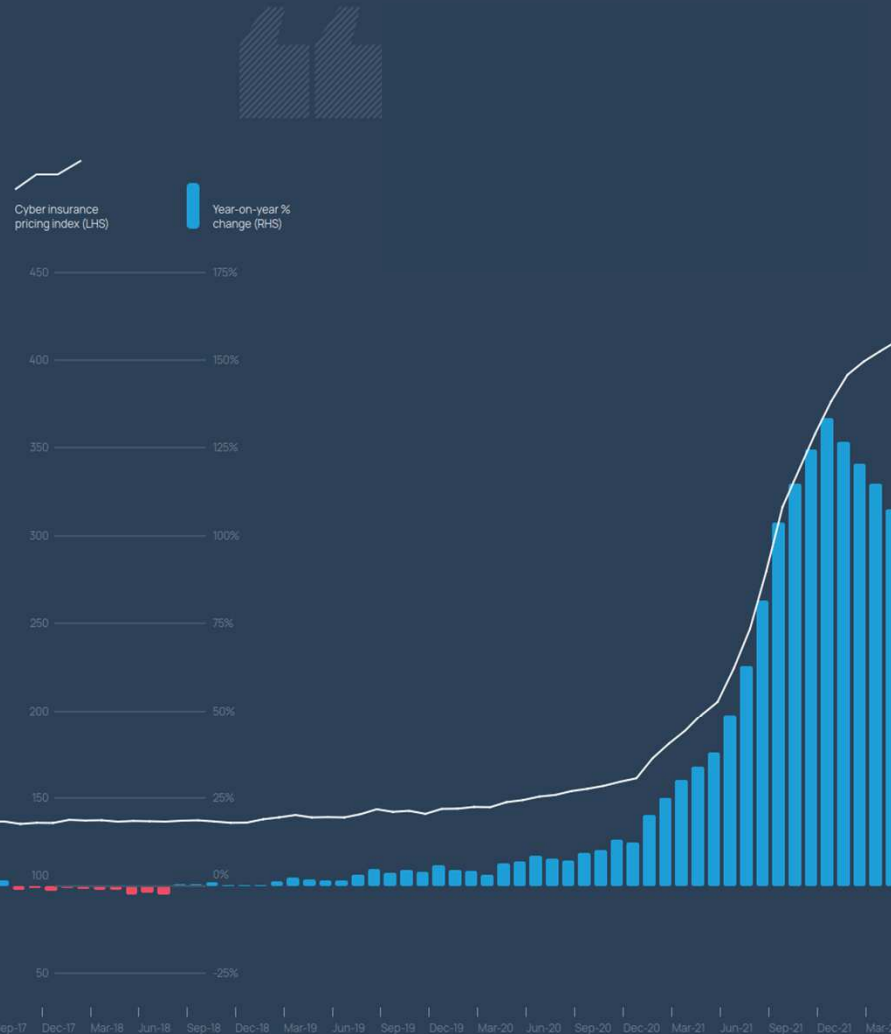
How these dynamics play out for the rest of the year will be instrumental in shaping the pricing environment. For the best part of a year, cyber has experienced the most extreme rate increases across the entire insurance market. The degree of repricing is visualised by Figure 20, which shows Howden's real-time, global cyber insurance pricing index, along with average year-on-year rate movements, dating back to 2014.

After a period of relative stable pricing through much of the last decade, a correction started to materialise in 2020, accelerating rapidly into a hard market set apart by a prolonged period of double- or triple-digit rate increases. Pricing today is approximately 300% higher than back in 2014, and the last eight months have seen 100% plus year-on-year rate changes. The last two full quarters (4Q21 and 1Q22) saw average annualised increases in excess of 120%, according to Howden data. The most current pricing data point prior to release of this report (April 2022) had year-on-year rate change at an average of +105%.

There are nevertheless signs that nascent rate moderation could transition into stabilisation towards the end of this year. The degree of repricing, coupled with tighter coverage terms, supported carriers' performance in 2021. And with robust risk controls starting to take hold and manifest into reduced claims activity, the ingredients are now in place for a return to profitability, absent any major escalation in the Ukraine war in particular. As difficult as the correction has been for companies, everyone benefits from a more mature market.

Clients will therefore be expecting a more rational cyber market to emerge later this year and into next, with access to capacity that rewards their improving risk profiles. Whilst the market remains difficult, pricing increases are likely to relent during the second half of 2022. Differentiated risk transfer and risk management advice can make a difference in such an environment by leveraging data analysis and expert insights to secure the coverage businesses are seeking.

Figure 20: Global cyber insurance pricing – 2014 to April 2022 (Source: NOVA)



# IL MERCATO ASSICURATIVO CYBER

## Le tendenze

### UTILIZZO DELLE POLIZZE IN AUMENTO

I dati del mercato assicurativo globale indicano un tasso di utilizzo per l'assicurazione cyber (percentuale di clienti che scelgono la copertura) in forte aumento.

### PREMI IN FORTE AUMENTO

Premi più alti hanno coinciso con un incremento della domanda e con maggiori oneri derivanti dai più frequenti e gravi attacchi informatici. In un recente sondaggio, più della metà dei clienti ha dichiarato di aver visto i prezzi aumentare del 50-150% alla fine del 2021.

### LIMITI DI COPERTURA INFERIORI E FRANCHIGIE MAGGIORI

La crescita del numero di attacchi informatici ha portato gli assicuratori a ridurre i massimali e i sotto limiti in tutti i settori e ad elevare le franchigie economiche e temporali.

### POLIZZE SPECIFICHE

Sempre più spesso gli assicuratori offrono polizze specifiche (stand alone) per il rischio informatico, piuttosto che includere tale rischio in pacchetti con altre coperture. Tale cambiamento riflette l'obiettivo di maggiore chiarezza su ciò che è coperto e di più rigorosi limiti di copertura specifici per il rischio cyber.

### MANCANZA DI DATI STORICI SULLE PERDITE

Senza dati completi e di alta qualità sulle perdite, può essere difficile stimare i potenziali danni dovuti agli attacchi informatici e, di conseguenza, le politiche di prezzo. C'è ancora poca collaborazione tra l'industria assicurativa e le Autorità nazionali per raccogliere e condividere i dati sugli incidenti al fine di valutare il rischio e sviluppare prodotti assicurativi cyber.

### MANCANZA DI DEFINIZIONI COMUNI E DI STANDARD COMUNI TRA LE COMPAGNIE

Le definizioni diverse di termini contrattuali, come "terrorismo informatico", possono portare a una mancanza di chiarezza su ciò che viene incluso in polizza. Le Autorità e il settore assicurativo potrebbero lavorare in collaborazione per promuovere definizioni comuni.

# IL MERCATO ASSICURATIVO CYBER

## Prospettive di crescita

### RILEVAZIONE POLIMI 2021 - ITALIA

- Solo il **27%** delle aziende italiane è protetto da una **polizza** cyber
- il **35%** sta ancora **valutando** come procedere
- Il **38% non ha** alcuna **intenzione** di sottoscriverla, o addirittura ne ignora l'esistenza

### ANALISI ASSITECA-HOWDEN 2022 5.000+ AZIENDE

- Aziende **con polizza** cyber ed e-crime: **10%** (500)
- Aziende **indecise** o **non intenzionate**: **50%** (2.500)
- Aziende **non «appetibili»** per il mercato: **40%** (2.000)

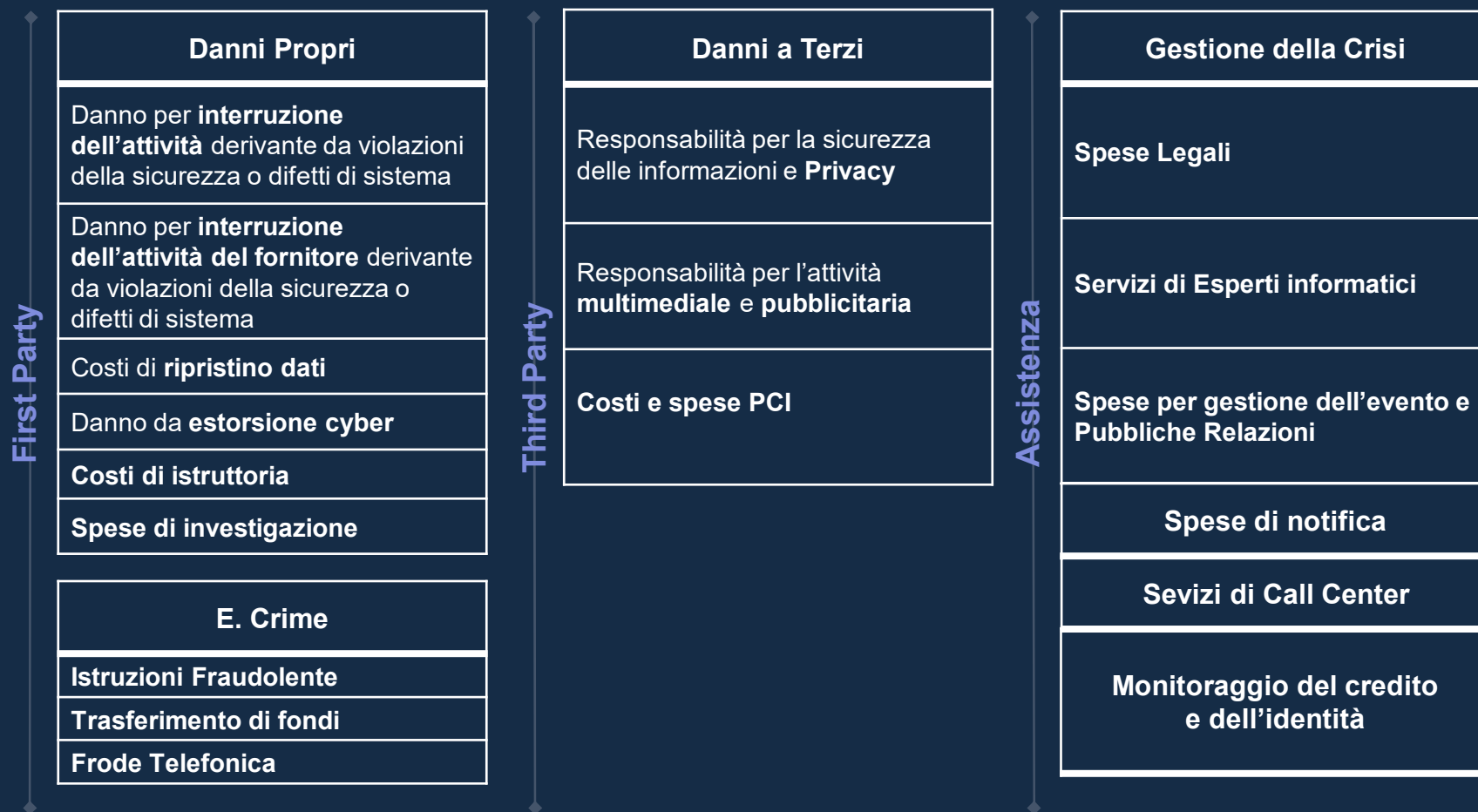
### PRINCIPALI PLAYER ITALIA

- |   |         |   |         |   |                 |   |          |   |        |
|---|---------|---|---------|---|-----------------|---|----------|---|--------|
| • | AIG     | • | Beazley | • | Gruppo Generali | • | Vittoria | • | Intesa |
| • | Allianz | • | Chubb   | • | Reale Mutua     | • | Zurich   | • | Etc.   |
| • | AXA     | • | Dual    | • | Unipol          | • | Satec    |   |        |



# COME FUNZIONA UNA POLIZZA CYBER

## Le principali coperture



# COME FUNZIONA UNA POLIZZA CYBER

## Le principali coperture

### RISCHI COPRIBILI

#### COMPUTER CRIME

Tutela i **fondi** dell'assicurato eventualmente distratti da un hacker (terzo)

Possibilità di estensione alle **merci**.

**Danno coperto:** valore di rimpiazzo del denaro o dei titoli (o delle merci) indebitamente trasferiti.

#### FRODE DA INGEGNERIA SOCIALE - SEF

Trasferimento di **fondi** a seguito di frode (buona fede del dipendente)

**Danno coperto:** valore di rimpiazzo dei fondi indebitamente trasferiti.

#### VOLUNTARY SHUTDOWN

**BI** operativa anche in caso di arresto volontario dei sistemi per motivazioni ragionevoli.

**Danno coperto:** Perdita di Profitto, Spese Extra (maggiori costi).

#### DANNI ALL'HARDWARE

Tutela il **patrimonio informatico fisico** dell'assicurato

**Danno coperto:** danno materiale e diretto alle cose (pc/server/stampanti/schermi/mobile devices) - (2 tipologie di trigger: solo cyber perils / qualsiasi evento).

#### TELEPHONE HACKING

Tutela le eventuali frodi a danno del **sistema di telecomunicazioni** aziendale.

**Danno coperto:** importo fatturato per telefonate non autorizzate o larghezza di banda non autorizzata.

Principali estensioni

### RISCHI NON COPERTI

#### SINISTRI NON COPERTI

I sinistri che presumono, si basano su, derivano da o sono attribuibili a **interruzione della rete o guasti** che non dipendono da infrastrutture sotto il controllo operativo dell'Assicurato.

**Guerra, terrorismo, sciopero.** La presente esclusione non si applica ad Atti di Cyber terrorismo che danno origine a un Sinistro.

**Furto di denaro o titoli** (Eccetto estensione «Crime» e «SEF»).

#### DANNI PROPRI NON COPERTI

Danni **materiali ai beni** (eccetto estensione «Danni Hardware»).

Danni che presumono, si basano su, derivano da o sono attribuibili alla **normale usura** o al graduale **deterioramento** dei Dati, ivi compresi dei mezzi di elaborazione dati.

Danni che presumono, si basano su, derivano da o sono attribuibili ad **azioni di un'autorità pubblica o del governo**, ivi compreso il sequestro, la confisca o la distruzione del vostro Sistema informatico o dei Dati.

Principali esclusioni

# IL PROCESSO SECONDO ASSITECA-HOWDEN

## Processo di acquisto di una polizza cyber nel 2023

### 1) CHECK UP

- Valutare preliminarmente le misure di sicurezza e le procedure adottate dall'azienda per ridurre i rischi informatici.
- Verificare la presenza dei requisiti minimi richiesti dal mercato assicurativo per ottenere una polizza Cyber e E-Crime.
- Sugerire eventuali approfondimenti e/o interventi.
- Modalità: intervista in video conferenza con il Responsabile IT e con il Referente assicurativo.

### 2) QUESTIONARIO GENERALE ASSITECA

- Sintesi aggiornata delle informazioni richieste da tutti gli operatori del mercato.
- Permette di definire il profilo generale di rischio dell'azienda.
- Contiene commenti sul contesto e i programmi dell'azienda.

### 3) GARA (VERIFICA DEL MERCATO)

- Le compagnie sono invitate ad una gara e il profilo dell'azienda è sottoposto al mercato, in base alle sue caratteristiche ed alle preferenze delle assicurazioni.
- Rischio gara deserta! Oggi occorre integrare il bando con una relazione tecnica di dettaglio sulle misure di sicurezza IT dell'azienda.

### 4) APPROFONDIMENTI

- Questionari specifici (es. Ransomware, GDPR, IoT, etc.),
- Soggettività: richieste specifiche.
- Programmi di sviluppo cyber dell'azienda.

### 5) ANALISI PROPOSTE E DECISIONE AZIENDA

- L'azienda valuta le proposte e decide quale offerta sottoscrivere.

### 6) FORMALIZZAZIONE

- Sottoscrizione documenti tecnici e questionario finale.

### 7) ASSISTENZA

- Assistenza in caso di sinistro, rendicontazione, rimborsi.

### 8) RINNOVO

- Il ciclo ricomincia anche con la stessa compagnia, ogni anno.

# IL PROFILO DI RISCHIO CYBER

## I requisiti più vincolanti

1. **Segregazione** funzionale della rete con segmentazione dei sistemi tra **IT e OT** (sistemi informatici per la produzione industriale)
2. **Antivirus e EDR/XDR** installati su tutti gli endpoint e i server
3. Esistenza di una **procedura di risposta** agli incidenti informatici (Incident Management)
4. Esecuzione regolare di **Vulnerability Assessment** e relativi Remediation Plan
5. Utilizzo della **multi-factor authentication MFA** per accessi da remoto, utenti privilegiati; amministratori di sistema; account cloud
6. Gestione dei **software obsoleti** (se presenti) e dei **software OT** (Operation Technology)
7. Piano di **formazione** sulla sicurezza informatica e sul GDPR e regolari **test di phishing** e relativa formazione
8. Presenza di **backup sicuri offline o in cloud** e gestione e archiviazione dei **LOG**
9. Piano di **Disaster Recovery** e possibilmente anche **Business Continuity Plan**
10. **Procedure IT** formalizzate

# IL PROFILO DI RISCHIO CYBER

## Punti di vista differenti

### ASSICURAZIONI



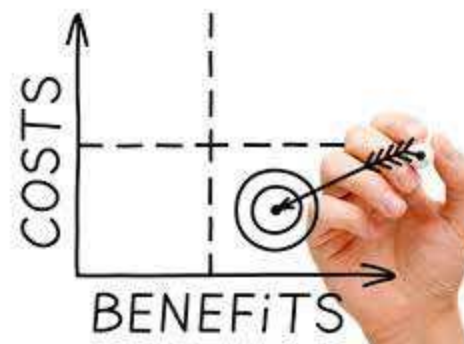
### IT MANAGER



### AZIENDA



### ASSITECA - HOWDEN



# IL RUOLO DEL MANAGEMENT

## Gli argomenti che dovrebbero essere sul tavolo di ogni CDA

1

### • Come verificare la postura cyber attuale

Verificare il livello di Governance, Competenze IT, Gestione della Sicurezza Informatica, Business Continuity e Crisis Management

2

### • Come sapere cosa è importante proteggere

Identificare il Patrimonio Informativo da proteggere. Esaminare il ciclo operativo e gli asset informatici da proteggere (HW, SW, Dati; Know How; Persone)

3

### • Come definire e guidare la difesa

Selezionare le misure di sicurezza in base al livello di maturità ed agli asset da proteggere. Sapere quali rischi si dovrà affrontare. Creare un sistema di controllo interno per indirizzare gli investimenti in base agli obiettivi ed alle performance

4

### • Come aumentare formazione e consapevolezza

Assicurare che i dipendenti, di qualsiasi livello, comprendano il valore e la sensibilità delle informazioni che trattano e il loro contributo nel proteggerle

5

### • Come migliorare monitoraggio e gestione Incidenti

Migliorare la capacità dell'azienda di monitorare i pericoli e di gestire gli incidenti informatici, in un panorama con rischi in continua evoluzione. Definire politiche, linee guida, procedure e criteri di valutazione per indirizzare la gestione della sicurezza e monitorarne le prestazioni

# CYBER SECURITY

## La responsabilità del Management: il quadro di riferimento

### Codice Civile

- Applicazione corretta delle regole di “Buona Governance”
- L’art 2381 stabilisce: “Gli organi delegati curano che l’assetto organizzativo, amministrativo e contabile sia adeguato alla natura e alle dimensioni dell’impresa”. La norma chiarisce che gli organi delegati curano l’adeguatezza degli assetti organizzativi, anche in materia di cyber sicurezza.

### Conformità

- D. lgs. 231/2001
- GDPR
- ISO 9001. etc.
- Le normative nazionali ed europee stanno convergendo in ottica di «Compliance Integrata»

### Normative di Settore

- Direttiva NIS n. 1148/2016 e NIS 2
- DPCM n.131/2020 e “DPCM2” sul perimetro di sicurezza nazionale cibernetica
- MDR (Medical Device Regulation), etc.

### Best practice internazionali

- ISO/IEC 31000, ISO/IEC 27001, COBIT, NIST, ENISA, Cyber Security Framework nazionale, ISO 22301, ecc.
- Sono tutte convergenti nell’individuare Chi, Cosa e Come deve gestire il rischio

# NEXT STEP 1: CHECK UP SICUREZZA INFORMATICA E POLIZZA CYBER

## Verifichiamo insieme il profilo di rischio dell'azienda

### Obiettivi:

- Supportare l'azienda in una **valutazione preliminare** delle **misure di sicurezza** e delle **procedure** adottate per **ridurre i rischi** informatici;
- **Verificare** la presenza dei **requisiti minimi** richiesti dal mercato assicurativo per ottenere una **polizza** sui rischi Cyber e E-Crime e il grado di «**appetibilità del rischio**»;
- **Suggerire** eventuali **approfondimenti** e/o interventi.

**Modalità:** intervista in video conferenza con il Responsabile IT e con il referente assicurativo. Le misure di sicurezza saranno discusse in base ad un framework specifico elaborato da Assiteca-Howden, che considera anche le richieste del mercato assicurativo, e riassunte in un report con eventuali suggerimenti.

	Essenziali	%	Importanti	%	Desiderabili	%	Totale	%
N° requisiti analizzati	10		23		27		60	
Soddisfatti o non applicabili	3	30%	7	30%	11	41%	21	35%
Parzialmente soddisfatti	0	0%	3	13%	7	26%	10	17%
Non soddisfatti o mancanza informazioni	7	70%	13	57%	9	33%	29	48%





# NEXT STEP 2: TEST DI PHISHING E FORMAZIONE UTENTI

## Aumentiamo la sicurezza delle aziende partendo dalle persone

Progettazione ed erogazione di campagne anti – phishing per verificare il livello di consapevolezza e conoscenza del personale e per sensibilizzarlo e formarlo a riconoscere questi pericoli e ad evitarli.

### OBIETTIVI

- ✓ Verificare il livello di attenzione e di preparazione degli utenti.
- ✓ Sensibilizzare e formare il personale a riconoscere ed evitare i tentativi di «phishing».
- ✓ Ridurre significativamente la possibilità di un attacco ransomware o di una truffa.

ANTI-PHISHING START	ANTI-PHISHING BASIC
<ul style="list-style-type: none"><li>✓ Esecuzione di 1 test di phishing iniziale per avere una base di partenza su cui progettare, eventualmente, ulteriori interventi.</li><li>✓ Erogazione di 1 modulo di formazione generale on-line.<ul style="list-style-type: none"><li>• Ogni utente potrà accedere, per 3 mesi, alla propria area riservata della piattaforma di training per visionare un video di circa 20'.</li></ul></li><li>✓ Invio di un report al termine del test di phishing e della campagna di formazione generale.</li></ul>	<ul style="list-style-type: none"><li>✓ Progettazione annuale delle campagne di phishing e della corrispondente formazione.</li><li>✓ Esecuzione di 2 test di phishing /anno.</li><li>✓ Erogazione di 3 moduli di formazione / anno.<ul style="list-style-type: none"><li>• Ogni utente può accedere alla propria area riservata della piattaforma di training per visionare i video di circa 20'.</li></ul></li><li>✓ Invio di report dettagliati al termine dei test di phishing e delle campagne di formazione.</li></ul>



Questo intervento è particolarmente **apprezzato dalle funzioni HR e dalle Autorità di Controllo** per le tematiche sulla Compliance al GDPR. Molte **Compagnie di Assicurazione** lo hanno inserito tra i prerequisiti per poter fornire coperture assicurative sui rischi cyber ed e-crime.

# NEXT STEP 3: GEI – GESTIONE EMERGENZE INFORMATICHE

## Organizziamo una reazione rapida ed efficace

**Assistenza specialistica in caso di incidente/attacco informatico.**

### Preparation

Attività preventive e preparatorie per migliorare l'efficacia dell'intervento in caso di incidente

- ✓ Definizione della procedura di gestione incidenti;
- ✓ Checkup delle procedure di backup e di LOG management;
- ✓ Checkup delle misure tecniche e organizzative richieste per la polizza cyber;
- ✓ Threat assessment (analisi esposizione azienda su internet) con test anti phishing, report e presentazione dei risultati.

### Crisis response (prime 48h)

Attivazione immediata di un *team di specialisti* (Incident Manager, Forensic Analyst, Cyber Legal, etc.) per aiutare il Top Management e il personale IT a *comprendere* rapidamente il tipo di incidente e la sua estensione;

Supporto nella *definizione delle attività* prioritarie (Piano di Remediation);

Assistenza nell'esecuzione degli interventi più urgenti.

### Remediation

Attività tecniche, specialistiche e/o professionali per il contenimento, la bonifica e la messa in sicurezza dei sistemi compromessi;

Supporto al ripristino dei servizi IT interrotti e monitoraggio;

Gestione di Data Breach, truffe e/o altri crimini informatici;

Indagini forensi.

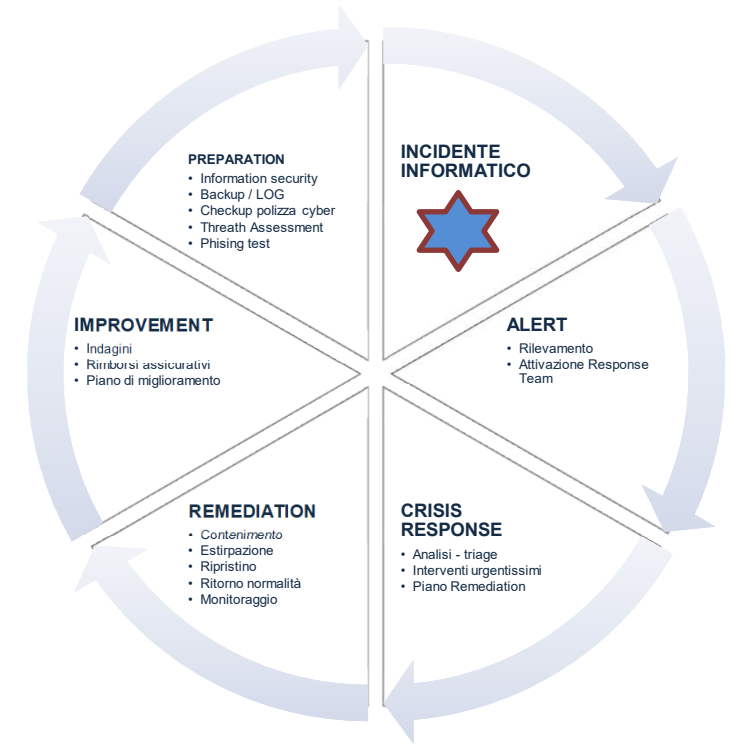
### Improvement

Supporto al ritorno alla normalità;

Assistenza legale;

Perizie e rimborsi assicurativi;

Piano di miglioramento della sicurezza e della resilienza IT.



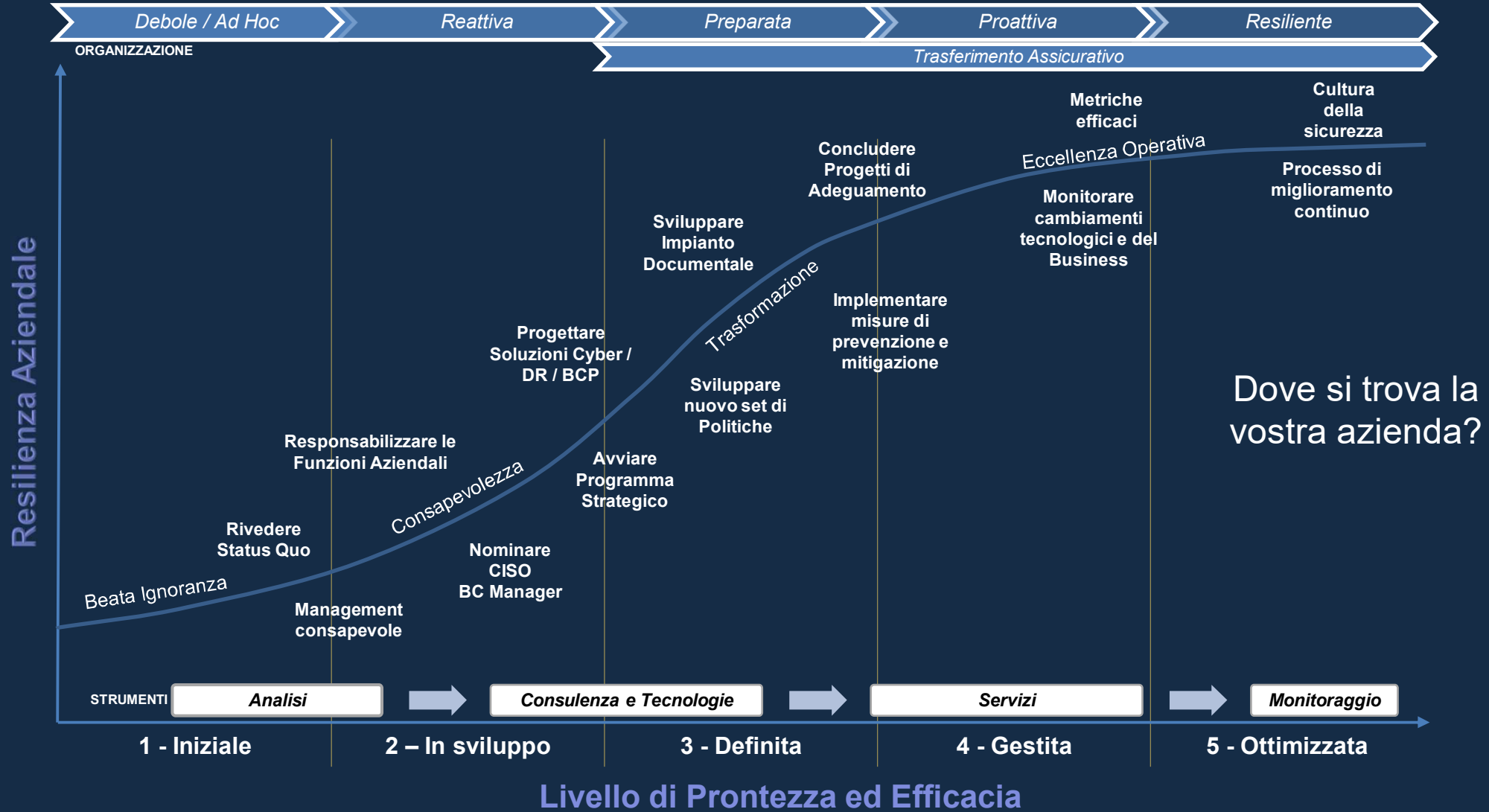
**Attivazione H24 7/7**

**800.936.036**

[gei@assiteca.it](mailto:gei@assiteca.it)

# CYBER SECURITY

## Verso il Cyber Risk Management



# CONCLUSIONI

## Diamoci una mossa

Il Cyber Risk cresce drammaticamente in frequenza e impatti.

È in definitiva una responsabilità del management e nessuna azienda dovrebbe sentirsi al sicuro.

Un approccio strutturato di gestione del rischio (Prevenzione - Protezione - Trasferimento) è la strategia più efficace.

Una solida postura cyber è essenziale anche per qualificarsi per la copertura assicurativa, al giorno d'oggi, ed è richiesto un supporto specializzato.

# Cosa ci guida?

## 1 Persone al primo posto

Tutto quello che facciamo è pensato dalle persone per le persone, perché anche nel business un rapporto solido e sincero è ciò che conta di più.

## 3 Prospettiva duratura

Fondiamo rapporti di fiducia e lealtà con i nostri clienti, basati su relazioni che durano nel tempo.

## 5 Network d'eccezione

Abbiamo colleghi e partner di fiducia in tutto il Mondo per fornire una visione internazionale.

## 7 Supporto tecnologico

Investiamo nel data&analytics per poter offrire soluzioni digitali a supporto delle decisioni strategiche di colleghi e clienti.

## 2 Indipendenza finanziaria


I nostri partner finanziari condividono progetti e valori permettendoci di seguire le esigenze dei nostri clienti senza vincoli.

## 4 Professionisti di valore

Mettiamo al servizio del cliente un team di esperti presenti sul territorio che lo supportino nell'analisi dei rischi e nelle decisioni strategiche.

## 6 Credibilità assicurativa

Il mercato assicurativo ci riconosce elevati standard di qualità, professionalità e puntualità ponendoci tra i primi player del mercato mondiale.



**Indipendenti per scelta.**

**Ambiziosi per vocazione.**

**Eccellenti per voi.**

# Howden in Italia



01.04.2021 - Nasce Howden Italia S.p.A.



26.07.2021 – Ingresso in Howden della Andrea Scagliarini S.p.A.



21.12.2021 – Ingresso in Howden di Tower S.p.A.



02.02.2022 - Ingresso in Howden di ASI Insurance Broker S.r.l.



01.04.2022 - Ingresso in Howden di Nord Est Insurance Broker S.r.l.



06.05.2022 - Ingresso in Howden di Assiteca S.p.A.



02.01.2023 - Ingresso in Howden di Assimovie S.r.l.

Il nostro percorso

# Howden Italia

## I numeri

€ 105 M

Ricavi 2022

€ 900 M

Premi 2022

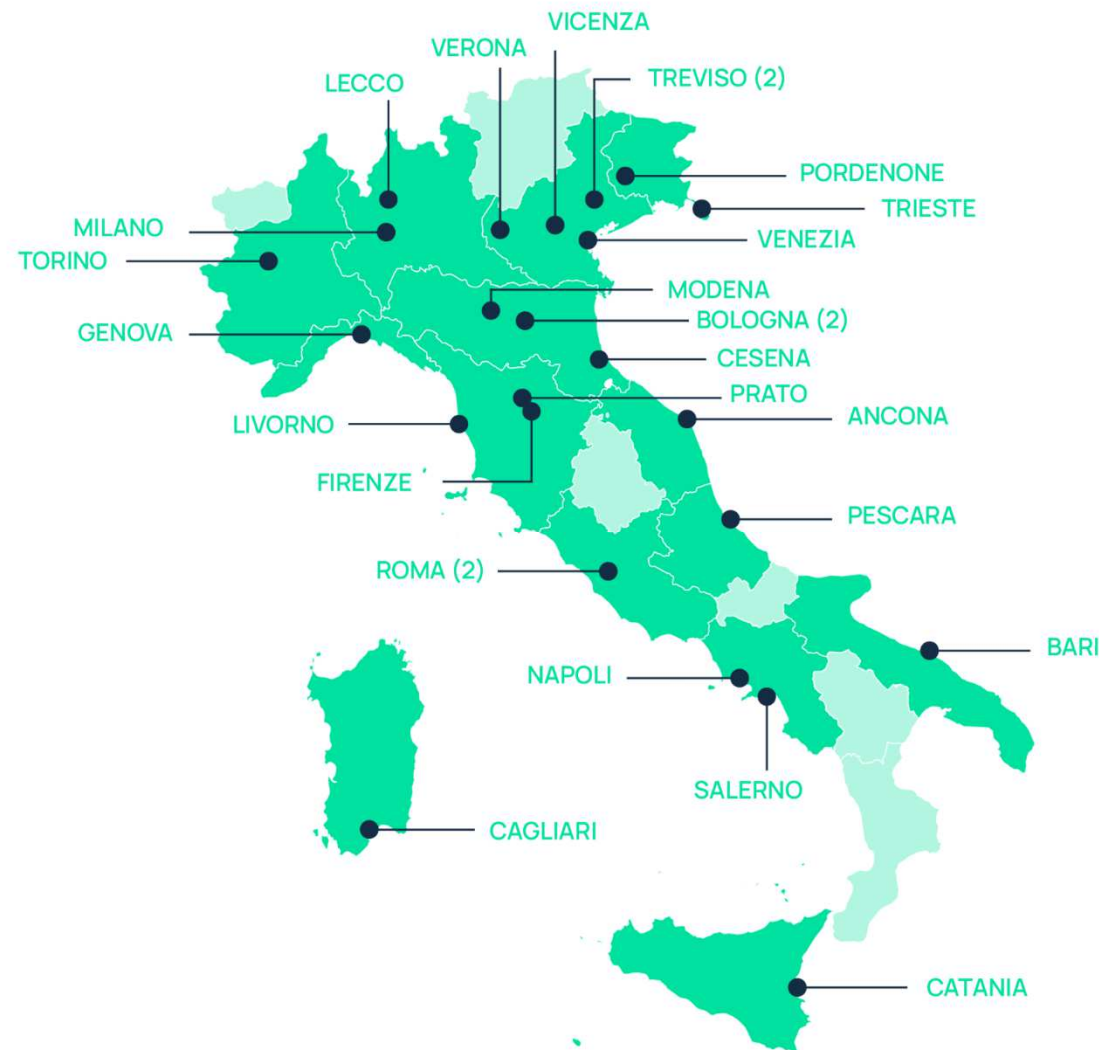
N°27

Uffici

+800

Persone

## 27 uffici in 24 città



**Emanuele Capra**

Responsabile Servizi di Consulenza

Cyber Security – Business Continuity

M +39 3493096530

[emanuele.capra@assiteca.it](mailto:emanuele.capra@assiteca.it)

Howden  
Italia S.p.A.

Sede legale  
Via Arconati 1  
20123 Milano

[howdenitalia.com](http://howdenitalia.com)  
[direzionecommerciale@howdengroup.com](mailto:direzionecommerciale@howdengroup.com)  
PEC [howden-italia@legalmail.it](mailto:howden-italia@legalmail.it)

P.iva  
IT11668410969  
RUI B000691645

This document or any portion of the information it contains may not be copied or reproduced in any form without the permission of Howden. Howden Italia S.p.A. is registered in Italy under VAT number 11668410969. Registered address: Via Arconati 1, 20123 Milano - Copyright © 2023