CONFINDUSTRIA VICENZA

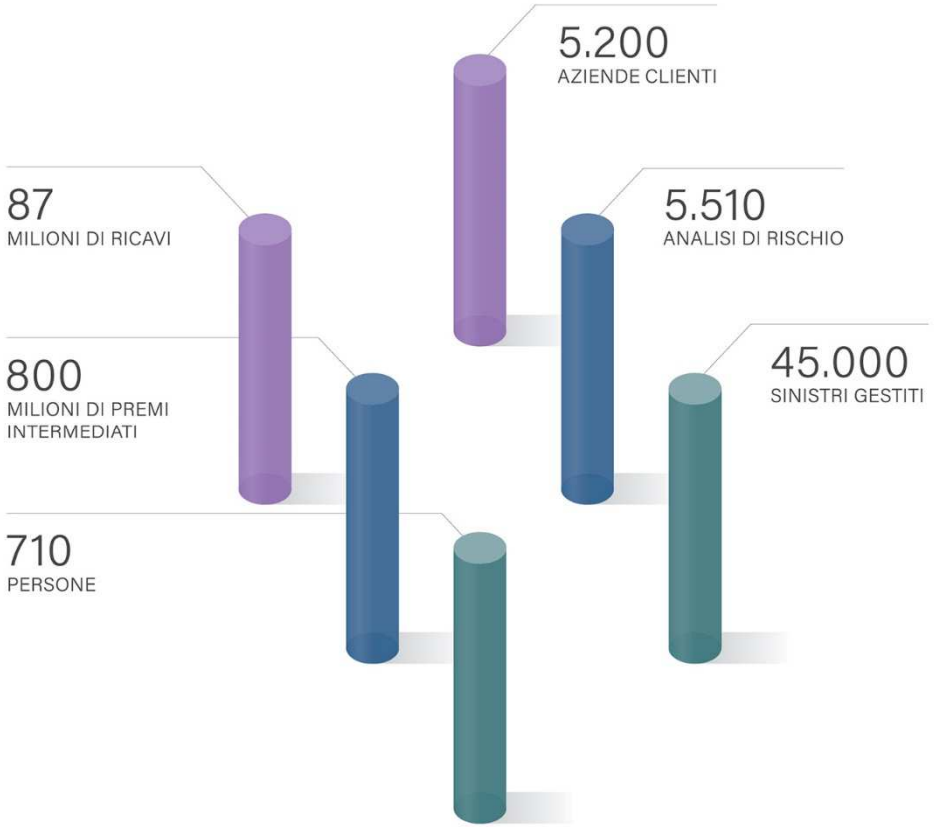
assiteca academy

**SICUREZZA CYBER**

Cosa fare per rendere la mia organizzazione più protetta e assicurabile

12 luglio 2022

ASSITECA è il più grande Gruppo italiano nella gestione dei rischi d'impresa e nel brokeraggio assicurativo.




**CERTIFICAZIONI**

- Certificazione di Qualità ISO 9001:2015 dal 1997
- Codice Etico e Modello Organizzativo 231/01 dal 2004
- Report di Sostenibilità
- Rating di legalità: ★★+

# LA NOSTRA METODOLOGIA DI LAVORO

ASSITECA adotta un approccio innovativo alla gestione dei rischi aziendali attraverso una metodologia di lavoro che integra analisi, consulenza e intermediazione.
Il nostro approccio parte dalla mappatura dei rischi, identificando le principali aree critiche e le priorità di intervento, per poi disegnare la struttura ottimale di gestione dei rischi e affiancare il cliente nel percorso di prevenzione, mitigazione e protezione.

**AGENDA**
***Le conseguenze pratiche degli attacchi informatici e le difficoltà del mercato assicurativo***

- Attacchi informatici: i **casi** più frequenti, gli **effetti** e le **attività** da implementare
- La gestione delle emergenze informatiche: cosa succede e **come gestire le prime 48 ore**
- La **visione del rischio** cyber dal punto di vista dell'azienda e dell'assicuratore
- **Come funziona la polizza** cyber
- Le **misure organizzative e tecnologiche minime** richieste per ottenere una polizza sui rischi cyber e e-crime
- Domande e commenti

# AZIENDE ITALIANE SOTTO ATTACCO
*I trend del settore*

## 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: 69

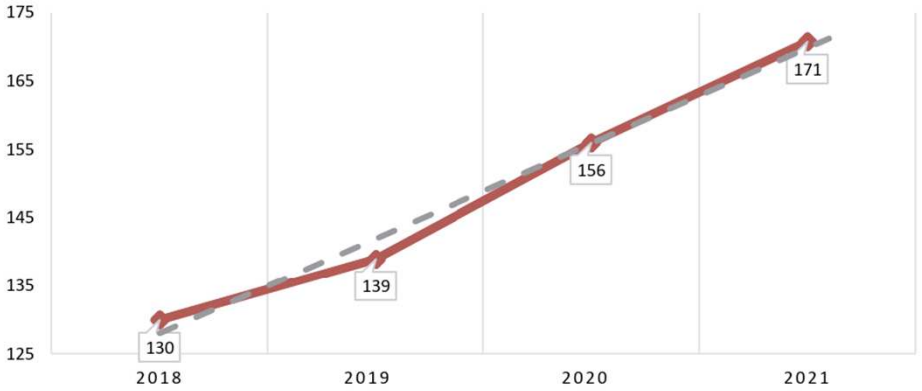
Figures don't add up to 100% as up to three risks could be selected.

| Rank | | Percent | 2020 rank | Trend |
|---|---|---|---|---|
| 1 | **Cyber incidents (e.g. cyber crime, IT failure/outage, data breaches, fines and penalties)** | **54%** | 2 (49%) | ▲ |
| 2 | Business interruption (incl. supply chain disruption) | **45%** | 1 (51%) | ▼ |
| 3 | Pandemic outbreak (e.g. health and workforce issues, restrictions on movement) | **28%** | **NEW** | ▲ |
| 4 | Natural catastrophes (e.g. storm, flood, earthquake, wildfire) | **25%** | 4 (20%) | = |
| 5 | Market developments (e.g. volatility, intensified competition/new entrants, M&A, market stagnation, market fluctuation) | **22%** | 5 (19%) | = |
| 6 | Changes in legislation and regulation (e.g. trade wars and tariffs, economic sanctions, protectionism, Brexit, Euro-zone disintegration) | **20%** | 5 (19%) | ▼ |
| 7 | Climate change/increasing volatility of weather | **19%** | 5 (19%) | ▼ |
| 8 | Loss of reputation or brand value (e.g. public criticism) | **13%** | 3 (29%) | ▼ |
| 9 | Fire, explosion | **10%** | 10 (12%) | ▲ |
| 10 | Critical infrastructure blackouts (e.g. disruption of power) | **9%** | **NEW** | ▲ |

## Severità % attacchi cyber 2018-2021


© Clusit - Rapporto 2022 sulla Sicurezza ICT in Italia

## Media mensile attacchi cyber 2018-2021

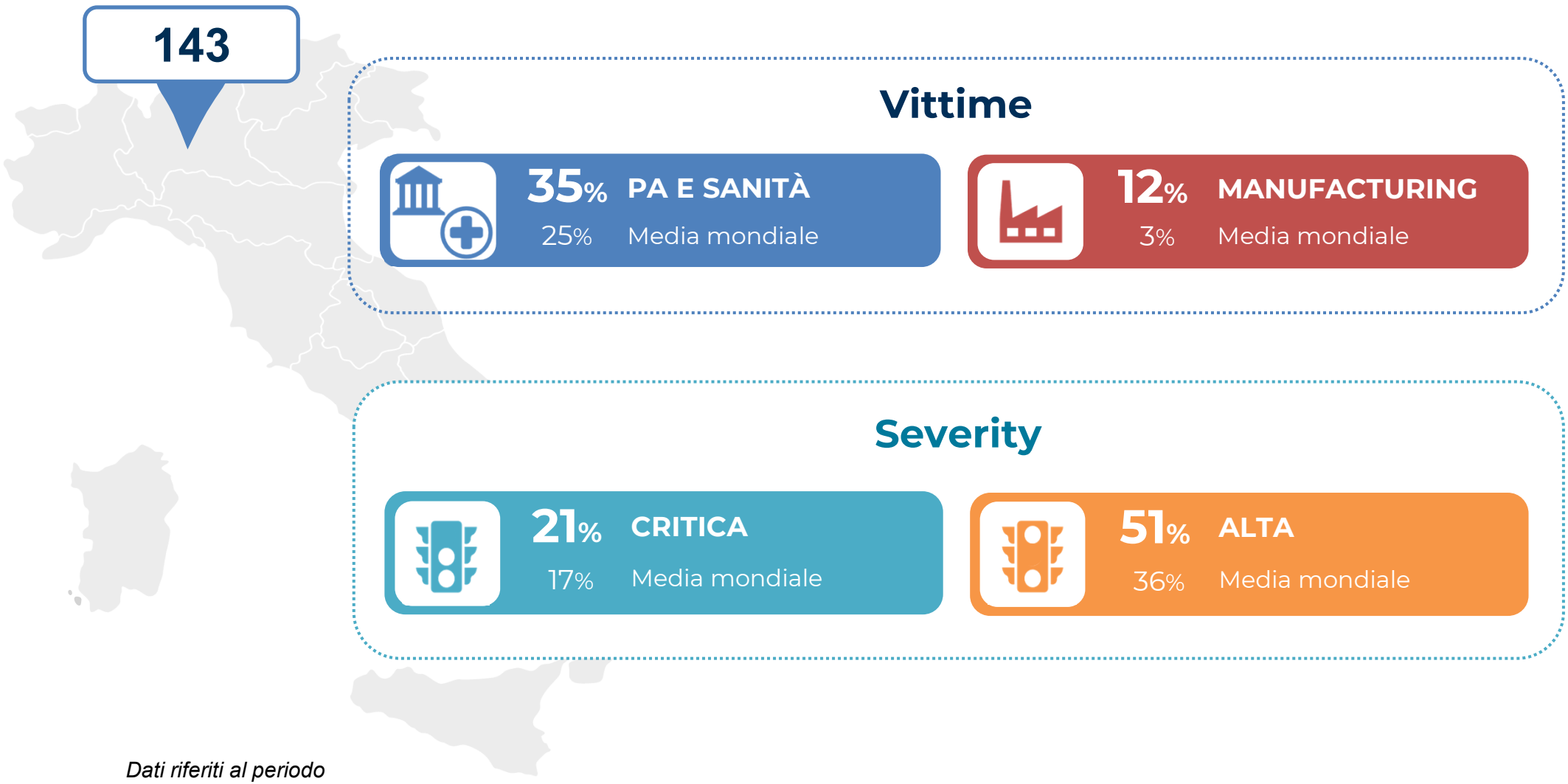



© Clusit - Rapporto 2022 sulla Sicurezza ICT in Italia

## Frodi indagate dalla Polizia Postale 2020-2021

| TIPO | 2020 | 2021 | INCREMENTO % |
|---|---|---|---|
| Numero di Frodi di interesse internazionale in danno di grandi e medio imprese investigate dalla Polizia Postale e delle Comunicazioni con l'ausilio della piattaforma F.I.S.A. – Financial Investigation Smart Analysis | 43 | 73 | 70% |

## AZIENDE ITALIANE SOTTO ATTACCO
*PA e Sanità al primo posto*




*Dati riferiti al periodo gennaio 2018 - giugno 2021*

# 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**

Si prevede che entro il 2031 i ransomware attaccheranno un'azienda, un consumatore o un dispositivo **ogni 2 secondi**, rispetto a un attacco ogni 11 secondi del 2021.

CYBERSECURITY VENTURES

* SOURCE: CYBERSECURITY VENTURES

# AZIENDE 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 mediani degli attacchi, in % sui ricavi, sono due volte e mezzo più alti perle 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 mediano di un attacco è aumentato del 29% a poco meno di 17.000 dollari.

HISCOX
Cyber Readiness Report 2022

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

# AZIENDE SOTTO ATTACCO
*Gli ultimi incidenti*

AZIENDE

SERVIZI

CYBERSECURITY360

**Il ransomware Conti colpisce anche Clementoni, nel bel mezzo dello shopping natalizio**

BY Dario Fadda

TGCOM24

CRONACA

26 OTTOBRE 2021 13:17

**Attacco hacker al gruppo San Carlo, il colosso delle patatine non paga il riscatto e denuncia**

A colpire il gruppo alimentare è stata la "gang" Conti, che ha all'attivo altri 400 attacchi informatici. Anche l'Iran nel mirino dei pirati, che hanno bloccato le stazioni di servizio locali

CORRIERE DELLA SERA ECONOMIA

Login

**Attacco informatico a Moncler, gli hacker chiedono un riscatto**

di Maria Silvia Sacchi

CORRIERE DELLA SERA ECONOMIA

Login


CYBER CRIME

**Campari, l'attacco hacker e il riscatto da 15 milioni di dollari: «Rubati i dati di 4.700 dipendenti»**

**Recanati: il manager della IGuzzini sull'attacco hacker subito dall'azienda**

radio_erre 14 Dicembre 2021 2

Non c'è pace per la IGuzzini Illuminazione oggi di proprietà del colosso svedese Fagerhult. Dopo la lunga trattativa sindacale, che si è conclusa in questi giorni con il licenziamento di 42 dipendenti, ora sono gli hacker a non far dormire sonni tranquilli al **manager, Cristiano Venturini.** Venerdì, infatti, dopo la Clementoni, gli hacker hanno preso di mira la vicina azienda iGuzzini mandando in tilt la rete informatica.

Cyber security


**Attacco hacker alla GEOX: colpite logistica e stoccaggio**

UtenzaDiServizioE-commerce News

25 Giugno 2020 Visite: 1597

CYBERSECURITYITALIA

Home ▸ News ▸ Italia ▸ Luxottica, produzione ferma e dipendenti a casa. Colpita da un attacco hacker?

Luxottica, produzione ferma e dipendenti a casa. Colpita da un attacco hacker?


LA STAMPA

**Attacco hacker: coinvolto il gruppo Miroglio di Alba**

L'azienda non colpita direttamente dal vasto assalto informatico a livello mondiale: problemi per un fornitore di software. Si lavora per ripristinare sicurezza e corretto funzionamento dei sistemi

A Motori

**Volvo Cars, attacco hacker al sistema informatico azienda**

Sottratti dati riservati del dipartimento Ricerca e Sviluppo

Redazione ANSA ROMA 13 DICEMBRE 2021 16:29

CYBERSECURITY360

**Bricofer, attacco ransomware e dati rubati: la nostra analisi**

BY Dario Fadda


il Resto del Carlino

MODENA EMILIA ROMAGNA ZONA

**Attacco hacker alla Fresenius Cyber criminali bloccano i pc**

Per diverse ore inaccessibili i dati della multinazionale Ma la rete di sicurezza ha poi respinto l'intrusione informatica

Pubblicato il 12 maggio 2020

**Attacco Ransomware al Gruppo Arcese**


tio 20 minuti

GRIGIONI 08.12.21 - 10:08

Aggiornamento : 11:34

**Hotel a cinque stelle vittima di un attacco hacker**

**I criminali informatici hanno colpito il Waldhaus di Flims, rubando dati di dipendenti e ospiti.**

FRIULIOGGI.IT

CRONACA

**Attacco hacker alla Eurolls di Attimis mette a rischio una commessa da 12 milioni**

Mercoledì, 23 marzo 2022

**Attacco hacker alle Ferrovie dello Stato, server paralizzati e treni a rischio**

L'azienda ufficializza in una nota l'attacco dei pirati ai sistemi informativi

JOURNAL

NEWS

**Hellmann Worldwide Logistics colpita da attacco informatico**

Una delle più grandi società di **logistica** al mondo ha subito un attacco informatico. Da un comunicato stampa

Cellulari.it

CURIOSITÀ

**Enel sotto attacco Hacker, 5 TB rubati: riscatto fissato a 14 milioni**

enel

A&E Rifiuti&Riciclo

Attacco hacker ai server Alia, è gestore rifiuti Firenze

Redazione ANSA FIRENZE 06 dicembre 2021 13:25

(ANSA) - FIRENZE, 06 DIC - Attacco di pirateria informatica al gestore dei servizi ambientali di Firenze e della Toscana interna Alia Servizi Ambientali spa che rende noto di "aver subito al propri server sono stati oggetto di un attacco informatico di natura dolosa" tanto che "si registra l'impossibilità di accedere al portale, ai relativi servizi digitali e a tutti i sistemi informatici".

ilriformista.it

**Hacker bucano Ho Mobile, ecco cosa devono fare i 2 milioni di clienti a rischio**

1 mese fa Giuseppe Mauro

Economia 24 ORE

ECONOMIA

**Un attacco informatico blocca i server della multiutility Iren**

di Filomena Greco

All'inizio di dicembre il sistema operativo della multiutility è finito nel mirino degli hacker. L'azienda: «Nessuna interruzione di servizi essenziali, presentata una denuncia alla procura di Genova, perché lì si trova il data center dell'intero Gruppo»

20 dicembre 2019

**Aruba: esposti alcuni dati anagrafici dei clienti**

- Stefano Regazzi 3 giorni fa

Con una email ai propri clienti, **Aruba** avvisa di aver subito un attacco hacker che ha esposto alcuni dati anagrafici. Il provider di servizi web (dall'hosting alla PEC) ha però fatto sapere che l'attacco, avvenuto il **23 aprile**, ha riguardato solo dei sistemi gestionali dell'azienda. Quindi i **server con i siti web dei clienti non sono stati attaccati.**

OPEN

TECNOLOGIA

**Attacco informatico a Sogin, la società che conserva le scorie nucleari: 800 Gb di dati in vendita per 250 mila dollari**

NOTIZIE TECNOLOGIA

**NOTO SERVIZIO VPN VITTIMA DI ATTACCO HACKER: IN VENDITA I DATI DI 69.400 UTENTI**

Di Francesco Santin | 2 Luglio 2021, ore 14:30

# ENTI PUBBLICI E ISTITUZIONI SOTTO ATTACCO
*Gli ultimi incidenti*

ENTI PUBBLICI

SANITA'

ISTITUZIONI

L'Arena

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

07 aprile 2022

LEAKED DATA

ENCRYPTED FILES ARE PUBLISHED

LA STAMPA

Il prezzo dell'attacco hacker? Alle casse del Comune di Rivoli è costato 30 mila euro

E' il denaro speso per riparare i danni dell'attacco informatico. Sono andati persi 4 giorni per il fermo dei servizi ai cittadini

PATRIZIO ROMANO

19 Marzo 2022 alle 13:13 | 1 minuti di lettura

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 BASILICI MENINI

12 Aprile, 2021

il Resto del Carlino

FERMO | PRIMO NATO | MUSEI APERTI

Home > Fermo > Cronaca > Attacc

Attacco hacker nell'archivio del Protocollo

La rete informatica del Comune è stata colpita di nuovo. Per fortuna i dati finiti nel mirino, dal 2000 al 2019, non sono stati persi

CORRIERE DELLA SERA BRESCIA

Login

CYBERSECURITY

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

di Massimiliano Del Barba

unionesarda.it

L'UNIONE SARDA.it

Il Comune di Guasila (foto Sirigu)

CRONACA SARDEGNA

Attacco hacker al Comune di Guasila: cancellati tutti i dati

Lunedì 24 Agosto 2020 alle 16:19

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

Redazione Corriere | 8 Novembre 2021

Ultimo aggiornamento 8 Novembre 2021 | 0

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*

TGCOM24

Accedi

02 MAGGIO 2022 19:31

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

Cybersecurity, sotto attacco 24% strutture sanitarie

Presentato il whitepaper di Sham e Università Torino, per il 54% delle strutture sanitarie rischio è percepito come una priorità

CARATTERISTICHE DEI RISPONDENTI

APPARTENENZA RISPONDENTI

TIPOLOGIA DI STRUTTURA

CAPIRE IL RISCHIO CYBER

LA VICENDA

17 gennaio 2022 - 11:47

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

di Gabriele Fusar Poli

il mattino

ACCEDI

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

*Nomi e cognomi, medici curanti, terapie e farmaci: è la stessa mano che ha colpito all'Usl di Padova. Riscatto non pagato*

Fabio Poloni

16 Gennaio, 2022

Sanità Toscana, hackerati i sistemi informatici

Non c'è pace per i sistemi informatici delle pubbliche amministrazioni di area sanitaria italiana. Gli hacker hanno capito che le difese sono facilmente "bucabili" e ci sguazzano.

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

Tweet

RANSOMWARE

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

BY Dario Fadda

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 sensibili appartenenti a diversi artisti, alcuni già in vendita sul dark web. L'associazione: «Non pagheremo»

Messaggero Veneto

ACCEDI

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

*Colpiti gli istituti di Sacile e Brugnera Marchesini, Della Valentina e Carniello. La denuncia del sindacato: «La rete è vulnerabile»*

Chiara Benotti

la Repubblica

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

*Cifrati i dati di docenti e allievi, compromessi oltre 100 computer a disposizione del personale. Il rettore: "Avviare contromisure per circoscrivere il danno, ripristinare dati e ricerche e assicurare il proseguimento della didattica"*

ROMATODAY

Politica

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'accatto"

Il Messaggero

FROSINONE

Foto e video sexy sui profili social, attacco hacker

TODAY Tech

Attacco hacker all'associazione bancaria: online dati sensibili

Bilancio Sampdoria, attacco hacker e addio soldi. Il caso

di Redazione

*La Sampdoria deve mettere un segno meno sul bilancio di 800mila euro a causa di un attacco hacker dalla 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.

RaiNews

Rai

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

# PMI SOTTO ATTACCO
*Le statistiche*

eritel
passione per l'ICT

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


B2BLABS
Startup 5G Trasformazione Digitale Intelligenza Artificiale Sicurezza Inforn

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

di Antonino Caffo
lunedì 26 luglio 2021 9:58
3 min vai ai commenti

Più informazioni su
Assiteca cybersecurity Cybersicurezza 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 soggetti 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
LETTURA: 4 minuti

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

(Foto Verizon Business)

TODAY

PARTNER

## Boom di attacchi informatici alle PMI

Negli ultimi 2 anni gli attacchi cyber sono aumentati del 246%: un problema rilevante

Un dato grave e preoccupante. Negli ultimi 2 anni il numero di **attacchi cyber** è cresciuto del 245% e nel 2014 si sono verificati circa 63.000 incidenti informatici in tutto il mondo. Colossi del calibro di JP Morgan, Sony e Dropbox non hanno passato un bel momento, ma il rischio di attacchi cyber non è solo una prerogativa delle grandi aziende. È una piaga che coinvolge soprattutto le aziende di piccole e medie dimensioni e gli studi professionali.

Cybersecurity, in Italia c'...
w-repubblica-it.cdn.ampproject.org

la Repubblica

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

*Il rapporto annuale del Clusit, l'Associazione italiana per la sicurezza informatica, sulla sicurezza informatica. Gli esperti: quella che emerge dai dati è "solo la punta dell'iceberg: le analisi si riferiscono ad attacchi reali, ovvero*

MENU 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


*I cyber-criminali provano a colpire questo target con la nuova variante del ransomware "eChoraix". Il risca coerente con i profitti.*

## 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.

# RISCHI INFORMATICI
*La mappa*

## ATTACCHI

- RANSOMWARE
- PHISHING
- MALWARE
- DDOS (DISTRIBUTED DENIAL OF SERVICE)
- SOCIAL ENGINEERING
- BEC (BUSINESS E-MAIL COMPROMISE)

## ATTORI

- CRIMINALI
- UTENTI NEGLIGENTI
- DIPENDENTI DISONESTI
- FORNITORI ICT
- SCRIP KIDDIE
- ATTIVISTI
- NAZIONI OSTILI

## RISCHI

**INCIDENTI (ERRORI / GUASTI)**
**INTERRUZIONE SERVIZI BLOCCO PRODUZIONE**
**FURTO / PERDITA DATI AZIENDALI / KNOW-HOW**
**ESTORSIONE**
**DATA BREACH (GDPR)**
**SPIONAGGIO / SABOTAGGIO**
**FURTO D'IDENTITÀ / FRODI**
**ATTACCHI DIMOSTRATIVI / CYBER WAR**

## MOTIVAZIONI

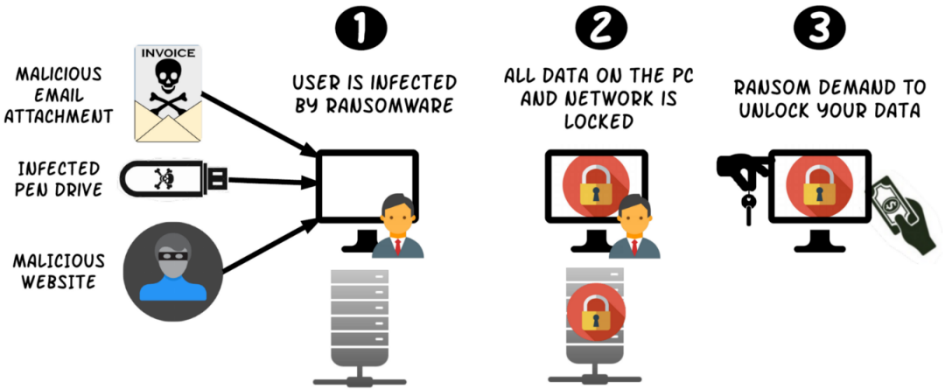
- DENARO
- FAMA
- CONCORRENZA SLEALE
- SPIONAGGIO
- POLITICA
- TERRORISMO

## VULNERABILITÀ

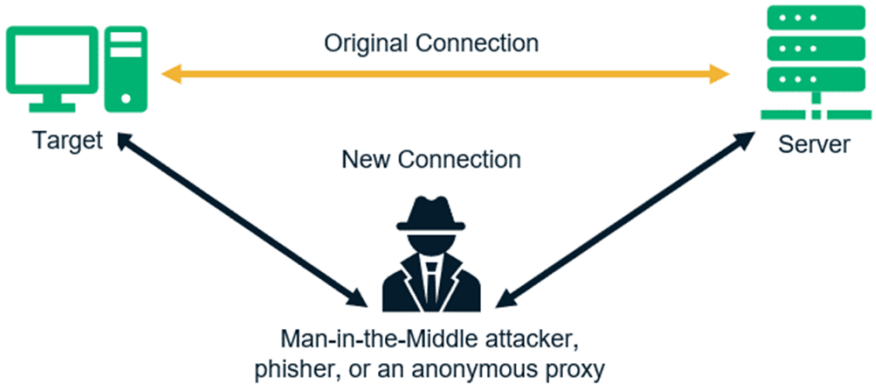
- SISTEMI OPERATIVI
- APPLICAZIONI
- TECNOLOGIE PRODUTTIVE (OPS TECHNOLOGIES)
- MANCANZA PROCEDURE
- SCARSA FORMAZIONE UTENTI
- FORNITORI

# ATTACCHI INFORMATICI
*I casi più frequenti rilevati da Assiteca*

## RANSOMWARE

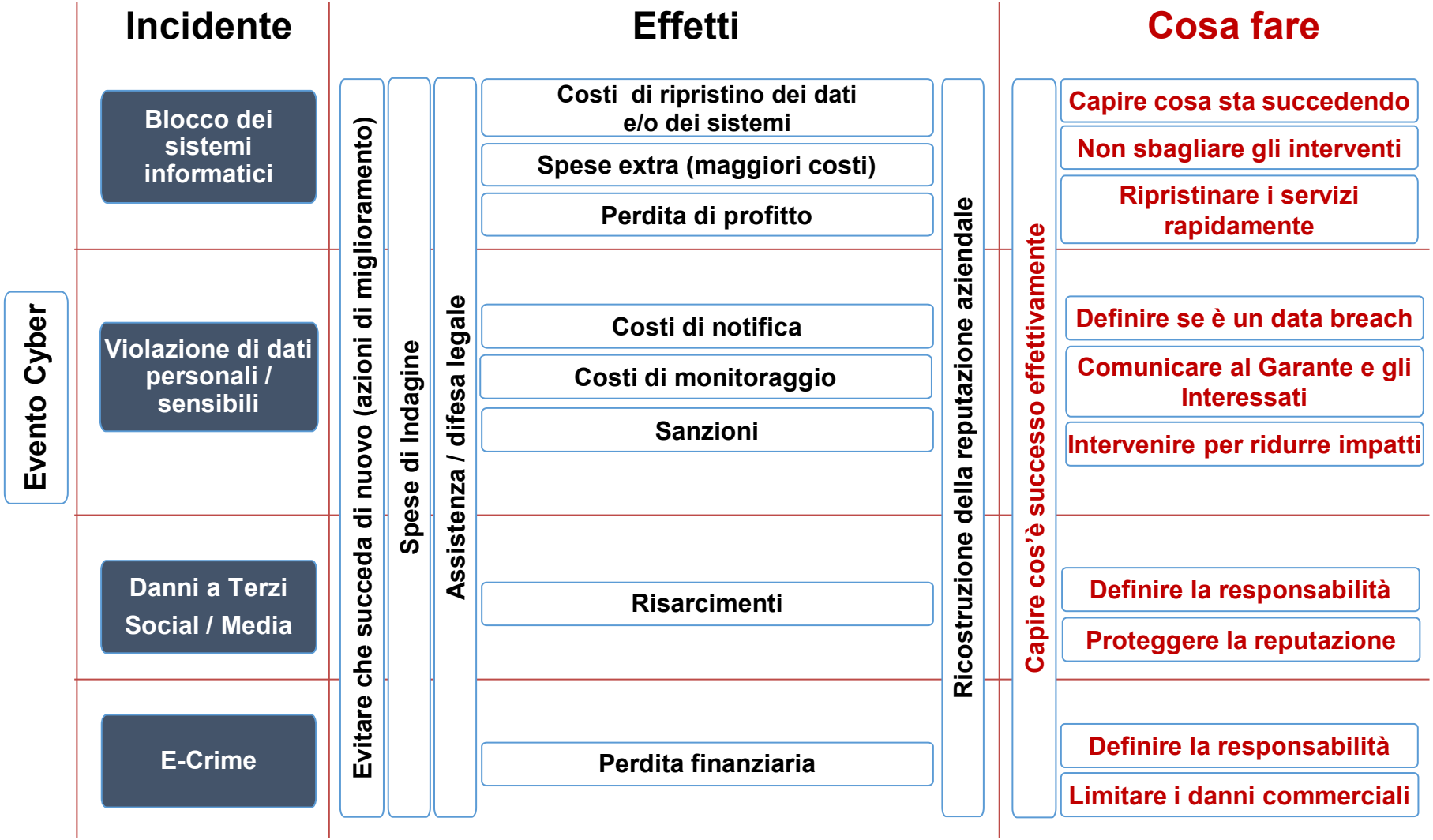



## TRUFFE




## ATTACCHI MIRATI

# ATTACCHI INFORMATICI
*Eventi - Effetti - Attività*



# GESTIONE EMERGENZE INFORMATICHE

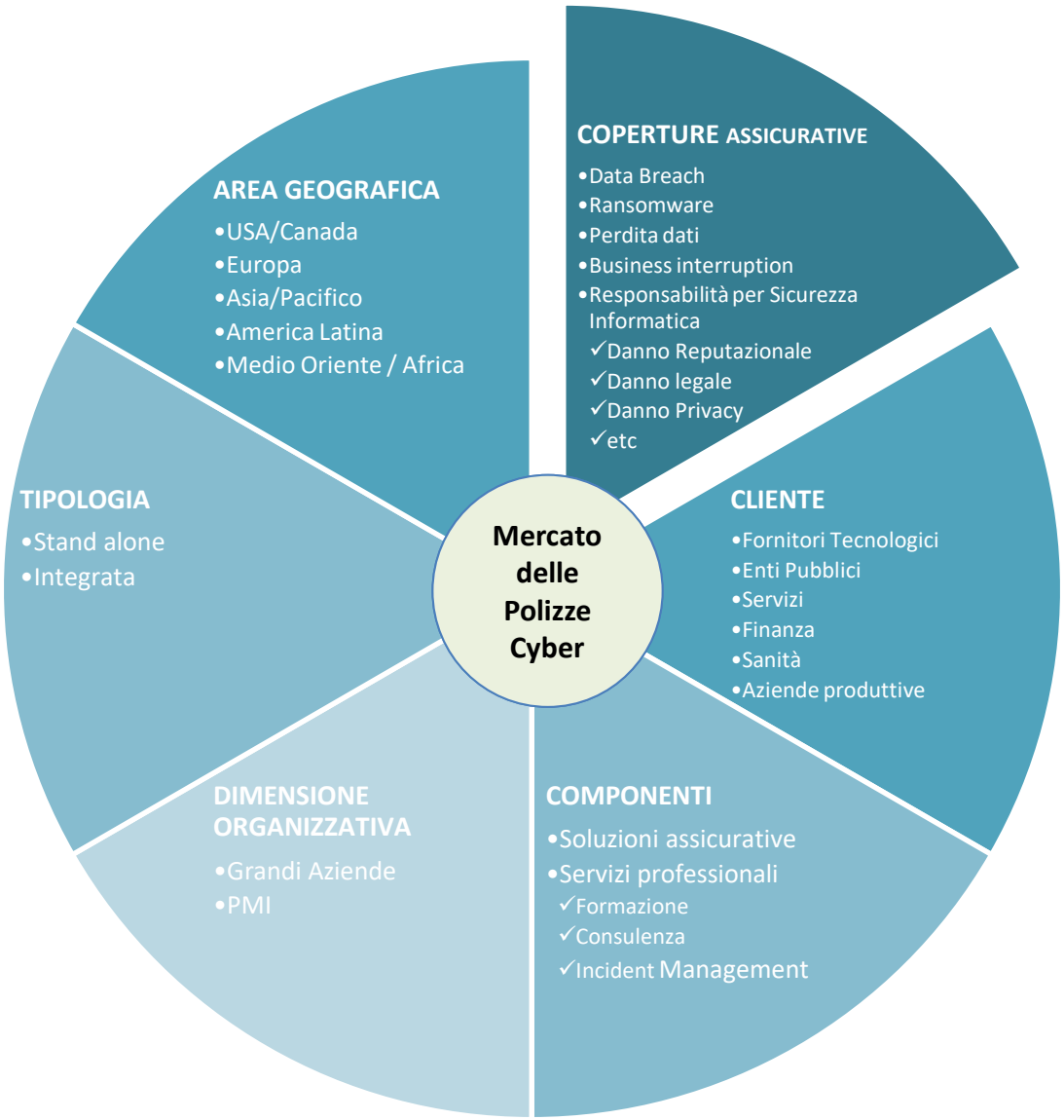
*Incidente informatico: cosa succede e come gestire le prime 48 ore*

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** |
| **PRIMO CONTATTO**<br>• Comprensione scenario<br>• Suggerimenti | **ANALISI SITUAZIONE**<br>• Riunioni/call con IT azienda<br>• Analisi dati e LOG (triage)<br>**DEFINIZIONE ATTIVITA'**<br>• Contenimento – Eradicazione – Ripristino<br>**INTERVENTI URGENTISSIMI** | **ATTIVITA' RIPRISTINO**<br>• Contenimento, bonifica, messa in sicurezza, ripristino e/o monitoraggio.<br>• Gestione Data breach, truffe e/o altri crimini informatici;<br>• Assistenza legale, indagini forensi, perizie | **ATTIVITA' POST CRISI**<br>• *Rimborsi assicurativi*<br>• Marketing e Comunicazione<br>• Assessment (organizzativo e VA)<br>• Piano di miglioramento (tecnologie e procedure)<br>• Monitoraggi dati on line |
| **OUTPUT**<br>• Allertare Manager e IT Team | **OUTPUT**<br>• Diario IT Manager<br>• Remediation Plan<br>  • Descrizione esiti, priorità ed approfondimenti,<br>  • Attività necessarie, professionalità richieste e tempistiche suggerite | **OUTPUT**<br>• Progettazione e esecuzione Interventi di ripristino<br>• Rapporti stato avanzamento | **OUTPUT**<br>• Rapporti indagini e danni<br>• Piano di miglioramento<br>• Implementazione tecnologie / procedure<br>• Rapporti monitoraggio on line |

# IL MERCATO ASSICURATIVO CYBER

*Una struttura sofisticata per rispondere a rischi complessi e dinamici*



# IL MERCATO ASSICURATIVO
*La situazione 2022/2023*

## MERCATO SPECIALIZZATO

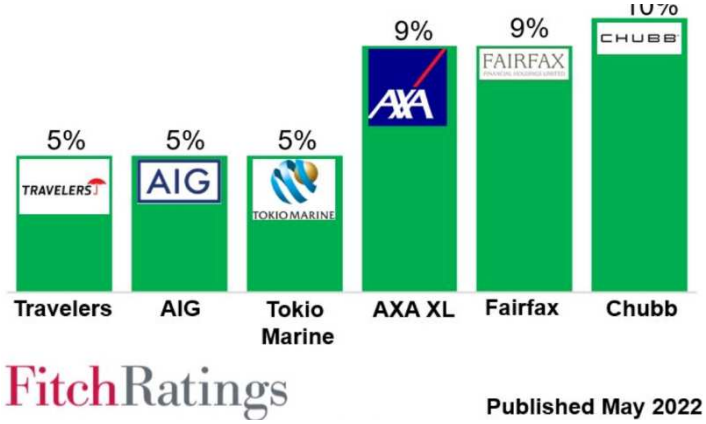
- **Numero limitato** di Compagnie Assicurative
- Assicuratori specializzati principalmente **stranieri**
- **Richieste informative sempre più ampie** sul rischio da assicurare.

## 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*



- **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.

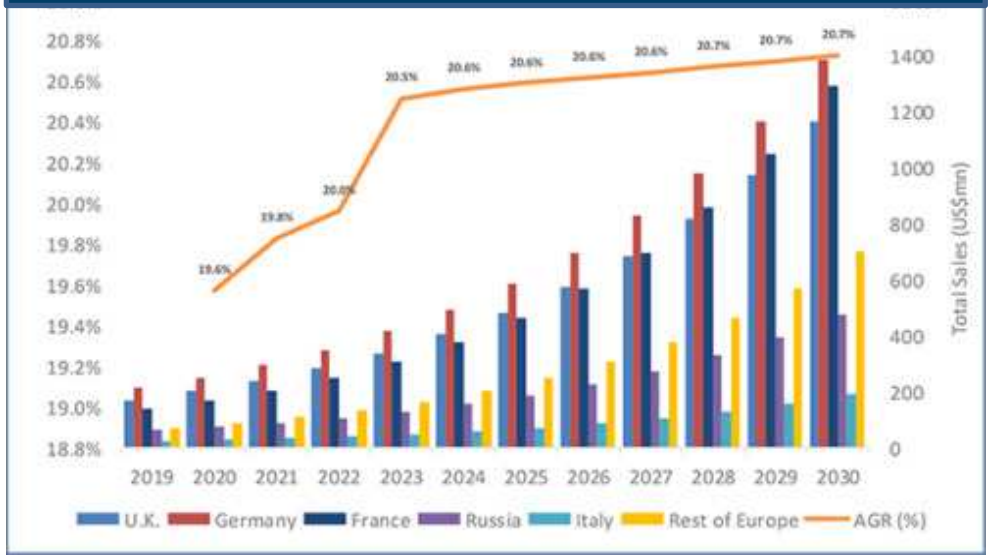
- **MANCANZA DI DATI STORICI SULLE PERDITE**
  Senza dati completi e di alta qualità sulle perdite, può essere difficile stimare i potenziali danni dovuti agli attacchi informatici e, di conseguenza, le politiche di prezzo. C'è ancora poca collaborazione tra l'industria assicurativa e le Autorità nazionali 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.

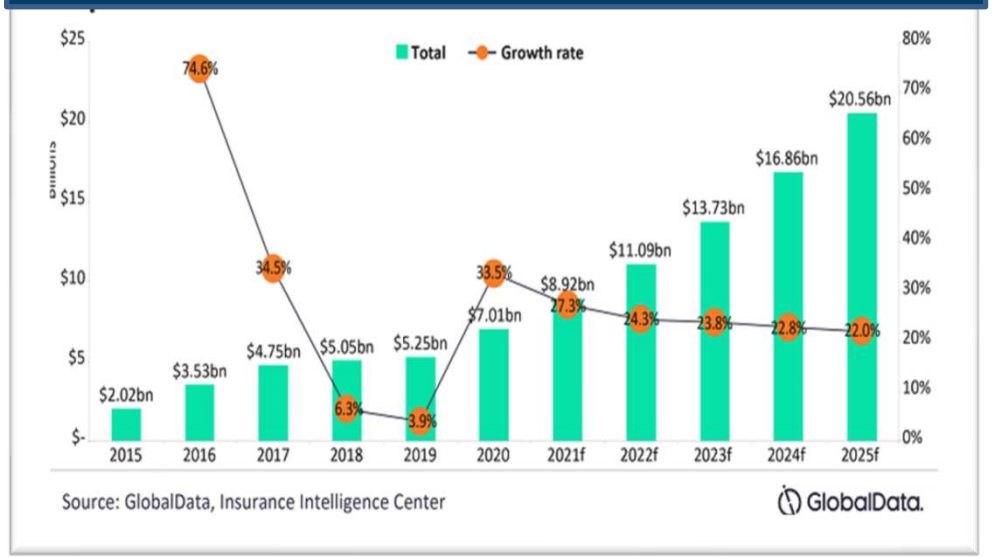
## PRINCIPALI PLAYER ITALIA

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

## PREVISIONI MERCATO **UE** 2020-2030 (US$m)




## PREVISIONI MERCATO **MONDIALE** 2025 (US$bn)



# IL MERCATO ASSICURATIVO
*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 2021 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)

# COME FUNZIONA UNA POLIZZA CYBER
*Le principali coperture*

## First Party

### Danni Propri

- Danno per **interruzione dell'attività** derivante da violazioni della sicurezza o difetti di sistema
- Danno per **interruzione dell'attività del fornitore** derivante da violazioni della sicurezza o difetti di sistema
- Costi di **ripristino dati**
- Danno da **estorsione cyber**
- **Costi di istruttoria**
- **Spese di investigazione**

### E. Crime

- **Istruzioni Fraudolente**
- **Trasferimento di fondi**
- **Frode Telefonica**

## Third Party

### Danni a Terzi

- Responsabilità per la sicurezza delle informazioni e **Privacy**
- Responsabilità per l'attività **multimediale** e **pubblicitaria**
- **Costi e spese PCI**

## Assistenza

### Gestione della Crisi

- **Spese Legali**
- **Servizi di Esperti informatici**
- **Spese per gestione dell'evento e Pubbliche Relazioni**
- **Spese di notifica**
- **Sevizi di Call Center**
- **Monitoraggio del credito e dell'identità**

# COME FUNZIONA UNA POLIZZA CYBER
*Le principali coperture*

## RISCHI COPRIBILI

Principali **estensioni**

### 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.

## RISCHI NON COPERTI

Principali **esclusioni**

### 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.

**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**.
- **Suggerire** 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.

## DESCRIZIONE DEL CONTESTO AZIENDALE

- Tipologia di business
- Dimensioni (fatturato, Italia/estero, n. siti, n dipendenti, controllate)

## DESCRIZIONE DEI SISTEMI INFORMATIVI

- Perimetro e dimensioni (data center, server, end point, etc.)
- Business on line (e-commerce/prenotazioni, accesso referti, siti dispositivi, pagamenti on line)
- Dati memorizzati e elaborati
- Utenti
- Organizzazione IT (interna/esterna, numero, etc.)
- Gestione account/utenze/credenziali/utenze amministrative
- Formazione del personale (training; regolamento, anti phishing)
- Responsabilità IT (AD, CFO, CIO, IT Manager)
- Utilizzo del Cloud (Office 365
- Sistemi di controllo industriale (SCADA, DCS, PLC, etc.)
- Dipendenza dai sistemi informativi (MTPD - quanto tempo senza prima di subire perdite economiche o reputazionali? % di impatto su attività operative?)
- Inventari (hardware, software, sistemi industriali)

**BACKUP**
- Procedura di backup giornaliero/settimanale/mensile/storico
- Luogo backup (cloud, off line, in rete, etc.)
- Test di ripristino

**PATCHING E SISTEMI OBSOLETI**
- Procedure di patching? Chi lo fa, quando, con che tecnologie

**SICUREZZA DELLA RETE**
- Firewall? IDS/IPS? ICS?
- Reti Guest
- Segmentazione rete
- Antivirus su server, pc? Filtri su proxy/gateway anti-malware?
- Email scanning?
- Monitoraggio? Strumenti/tecnologie? SOC interno/esterno H24?

**DEVICE PRIVATI E ACCESSI DA REMOTO**
- Da quali dispositivi? (notebook, smartphone, fornitori, consulenti, clienti)
- A quali servizi? (posta elettronica, CRM, ERP, etc.)
- Quali misure di sicurezza?

**DOCUMENTAZIONE**
- Policy e procedure (complete, scritte)
- Certificazioni (ISO 27001, ISO 22301, GDPR, Audit terze parti)

**AUDIT, INCIDENT RESPONSE E BUSINESS CONTINUITY**

- Vulnerability Assessment e Penetration Test
- Remediation Plan
- Procedura di gestione incidenti (specifica, scritta, anche per Data Breach GDPS)
- Piano di Disaster Recovery IT (soluzione tecnica, piano formalizzato, test)

**SISTEMA DI GESTIONE DELLA SICUREZZA**

- Risk Management (Policy, Piano formazione, Analisi Rischi / BIA, audit)
- Protezione sistemi informativi (MFA, gestione password, gestione profili utente, gestione configurazioni, antivirus/firewall, patch, backup, DRP)
- Sicurezza della Rete e delle operazioni
- Sicurezza fisica CED / Data Center
- Servizi in Outsourcing

**DATI PERSONALI**

- Tipo e numero record
- Politica protezione dati personali
- Trattamenti
- Controlli per la protezione dei dati personali

**SICUREZZA RANSOMWARE**

- Formazione antiphishing
- Segnalazione email esterne
- Procedura segnalazione mail sospette, spam
- Pre-visualizzazione allegati
- Filtraggio posta
- Filtraggio navigazione web
- Sandbox
- MFA per utenti, fornitori esterni, clienti
- Sicurezza endpoint (antivirus, monitoraggio, amministratore locale, porte usb)
- Archiviazione e monitoraggio dei LOG (archiviazione, sicura, monitoraggio interno, piattaforma, SOC)
- Credenziali privilegiate (AdS, registro, MFA, altre utenze)
- Gestione Active Directory (numero account dominio amministratori, numero account dominio utenze di servizio)

**SICUREZZA OT e IoT**

- Ambiente OT segmentato da IT (firewall, gateway, VLAN, DMS)
- Ambiente OT separato da internet
- Accesso a OT da remoto bloccato o regolamentato (dipendenti e fornitori)
- Inventario Asset OT
- Vulnerability Assessment OT
- EDS EDR SOC
- Backup Asset OT
- Sicurezza dei device IoT - Internet of Things

## I REQUISITI PIU' VINCOLANTI

1. **Segregazione** funzionale della rete
2. Segmentazione dei sistemi tra **IT e OT** (sistemi informatici per la produzione industriale)
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** per accessi da remoto, utenti privilegiati e amministratori di sistema
6. Gestione dei **software obsoleti** (se presenti) e dei **software OT** (Operation Technology)
7. Piano **di formazione** sulla sicurezza informatica e sul GDPR
8. Regolari **test di phishing** e relativa formazione
9. Presenza di **backup sicuri offline o in cloud**
10. Piano di **Disaster Recovery** e possibilmente anche **Business Continuity Plan**

**ASSICURAZIONI**


**IT MANAGER**


**AZIENDA**

**ASSITECA**

## 1) 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*.

## 2) Conformità

- D. lgs. 231/2001
- GDPR
- ISO 9001. etc.

Le normative nazionali ed europee stanno convergendo in ottica di «Compliance Integrata»

## 3) 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.

## 4) 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

## IL RUOLO DEL MANAGEMENT

***Gli argomenti che dovrebbero essere sul tavolo di ogni cda***

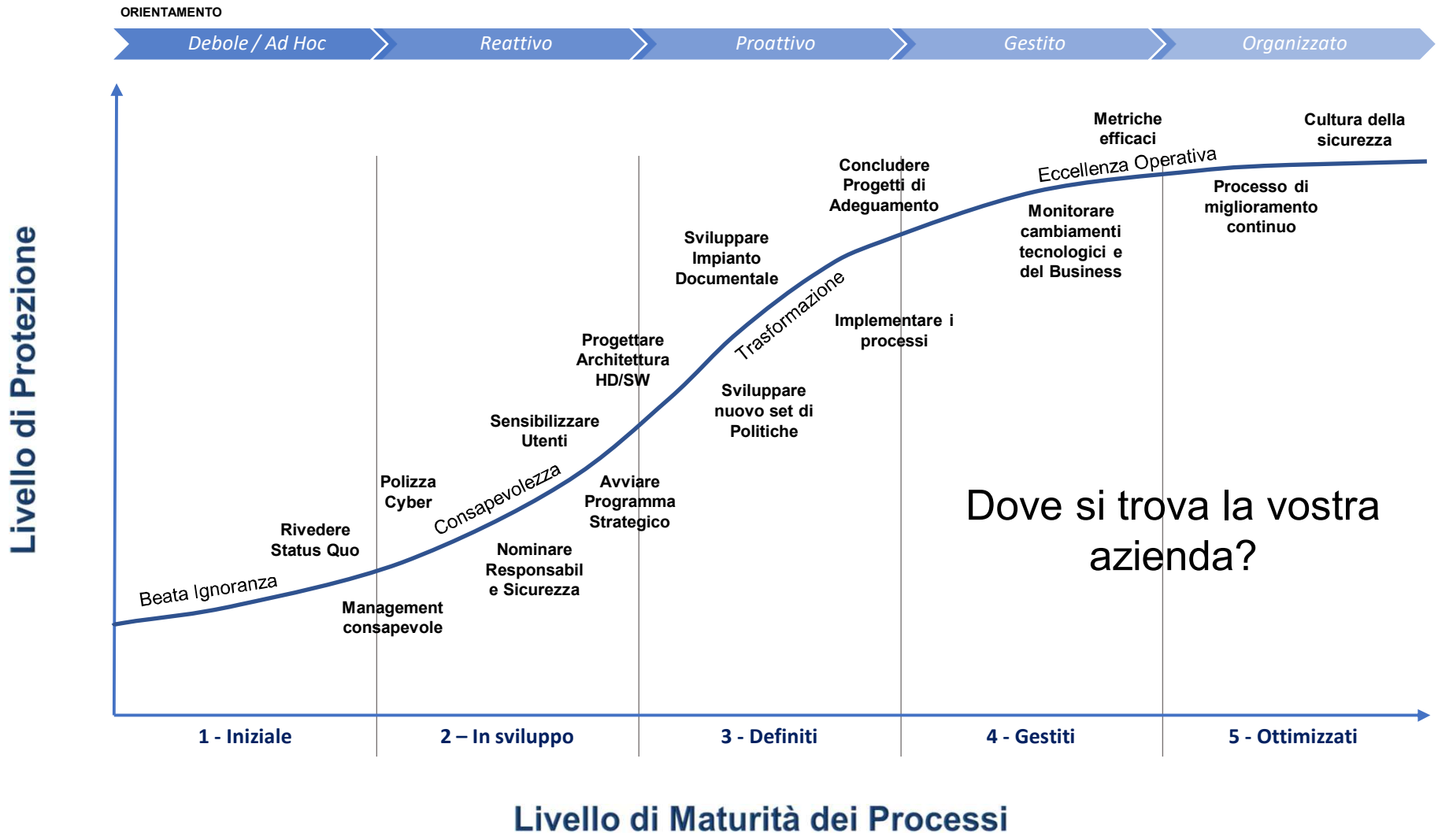
1. **Come verificare la postura cyber attuale**
   Verificare il livello di Governance, Competenze IT, Gestione della Sicurezza Informatica, Business Continuity e Crisis Management

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 aglio 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 lor 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


ORIENTAMENTO
Debole / Ad Hoc
Reattivo
Proattivo
Gestito
Organizzato
Livello di Protezione
Beata Ignoranza
Rivedere Status Quo
Management consapevole
Polizza Cyber
Consapevolezza
Sensibilizzare Utenti
Nominare Responsabile Sicurezza
Progettare Architettura HD/SW
Avviare Programma Strategico
Sviluppare Impianto Documentale
Sviluppare nuovo set di Politiche
Trasformazione
Concludere Progetti di Adeguamento
Implementare i processi
Eccellenza Operativa
Monitorare cambiamenti tecnologici e del Business
Metriche efficaci
Processo di miglioramento continuo
Cultura della sicurezza
Dove si trova la vostra azienda?
1 - Iniziale
2 – In sviluppo
3 - Definiti
4 - Gestiti
5 - Ottimizzati
Livello di Maturità dei Processi

# CONCLUSIONS
*Get a move on*

- 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.

**ASSITECA**
**www.assiteca.it**
Via Goffredo Sigieri, 14 - 20135 Milano

**Emanuele Capra**
Responsabile Rischi Operativi - Cyber Security
M +39 3493096530
emanuele.capra@assiteca.it

**Mirco Piccoli**
Account Executive
M +39 3401888618
mirco.piccoli@assiteca.it

# Come accrescere la «consapevolezza» in azienda sul tema cybersecurity

*Alessio Dichio - 12 luglio 2022*

*Diffidiamo dall'essere immuni e perfetti, sarà un bellissimo stimolo per creare percorsi di crescita, personali e aziendali, sia nell'ambito cybersecurity che nella vita.*

# Complessità sì, ma fino a un certo punto…

**33,6 mln (+101%)**

Minacce tramite email

**16,5 mln (+138%)**

Attacchi di phishing

*Fonte: Cloud App Security Threat report 2021*

*Trend Micro - confronto con 2020*

# Le minacce principali

### Phishing

email mirata all'ottenimento dei dati personali o professionali della vittima

### Spoofing

evoluzione del phishing perché il mittente è un indirizzo «conosciuto» (di solito con allegati malevoli)

# Awareness is the key!

- Traffico di email massiccio
- Popolazione aziendale variegata e poco digitalizzata
- Abuso di utilizzo della strumentazione aziendale per scopi personali

**FORMAZIONE!**

# Awareness

### Corsi continuativi

Le minacce evolvono, non può essere una tantum!

### Piattaforme specifiche

Grande varietà di soluzioni. Dall'e-learning base a veri e propri attacchi *fake*

### Per tutti!

Tutti devono partecipare. Dal top management ai dipendenti

### Sicurezza estesa

Le accortezze apprese valgono anche per i dispositivi privati!

### Competizione

Creazione di scoreboard per aumentare attenzione durante l'apprendimento

### Obiettivo

Instillare il *dubbio* prima di fare azioni su email sospette

# Insieme si vice

- La sinergia di contromisure riesce a proteggere le organizzazioni
- Avere un'infrastruttura aziendale all'altezza è un requisito fondamentale
- Procedure di backup & restore immediate limitano i danni
- Tutto ciò è propedeutico per una polizza cyber

# Grazie!

Ci sono domande?