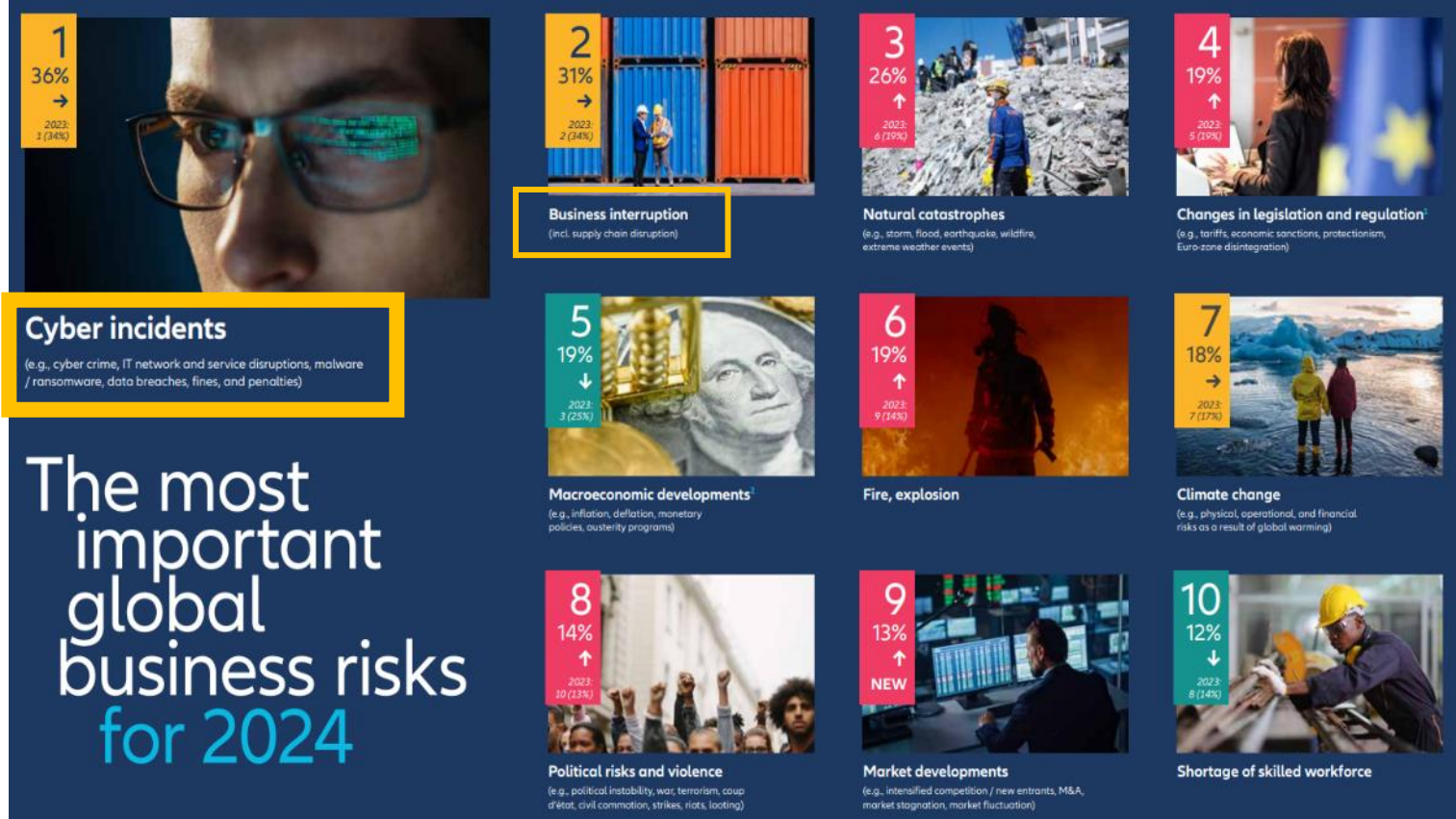


NIS2: l'analisi del rischio e la gestione degli incidenti

Il rischio «cyber» non è soltanto cyber

Federico Lucia

Amministratore Delegato Fortaris S.r.l.
Board Member e Direttore Didattico ANRA
Vicepresidente DFA



Un contesto in evoluzione | Il Global Risk Report del WEF

Global Risks Report 2025

Global risks ranked by severity

Severity ranking by stakeholder over the short term (2 years)



Risk categories: Economic (blue), Environmental (green), Geopolitical (orange), Societal (red), Technological (purple)

Source: World Economic Forum, Global Risks Perception Survey 2024-2025

Vista a 2 anni...

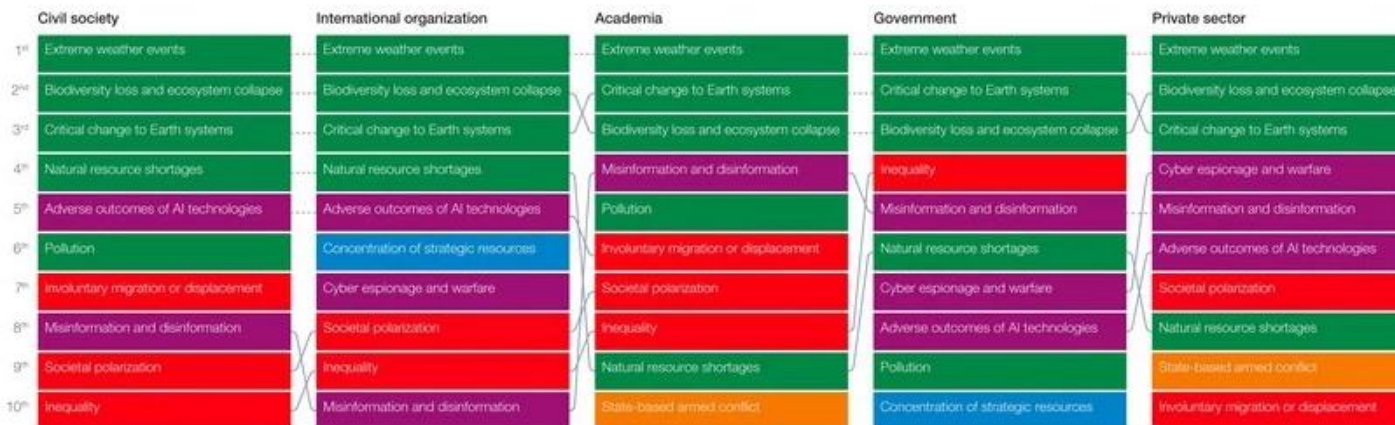
Un contesto in evoluzione | Il Global Risk Report del WEF

Global Risks Report 2025

Global risks ranked by severity



Severity ranking by stakeholder over the long term (10 years)

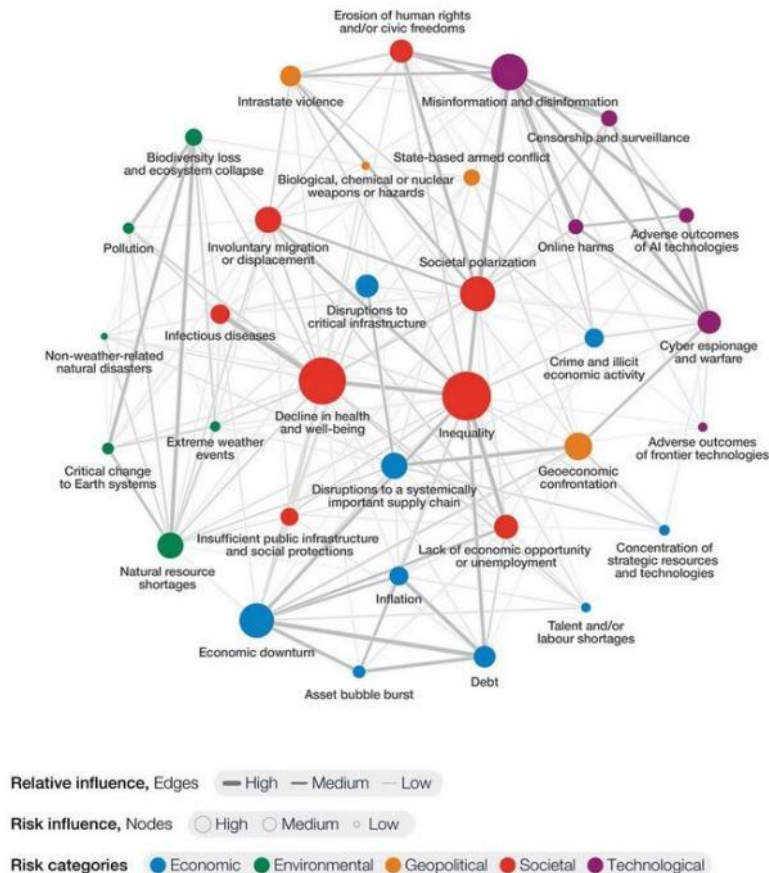


Risk categories: Economic (blue), Environmental (green), Geopolitical (orange), Societal (red), Technological (purple)

Source: World Economic Forum, Global Risks Perception Survey 2024-2025

... Vista a 10 anni

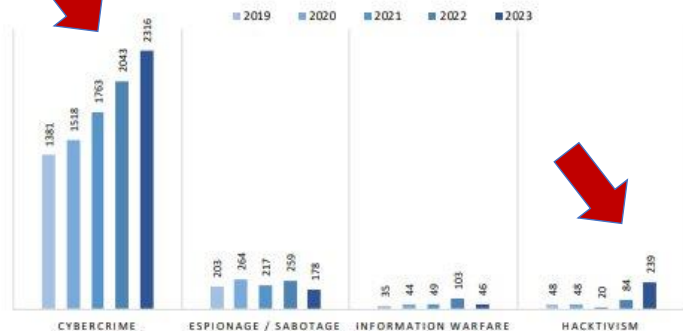
Un contesto in evoluzione | Il Global Risk Report del WEF



...e le interconnessioni tra i rischi

Un contesto in evoluzione | Il rapporto del Clusit 2019 - 2023

Attaccanti 2019 - 2023



© Clusit - Rapporto 2024 sulla Sicurezza ICT in Italia

Top 10 vittime in 2019 - 2023



Severity 2019 - 2023



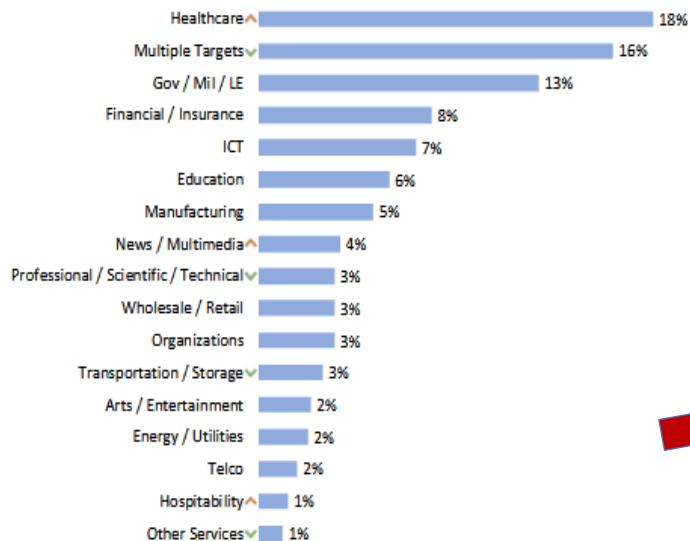
Tecniche di attacco 2019 - 2023



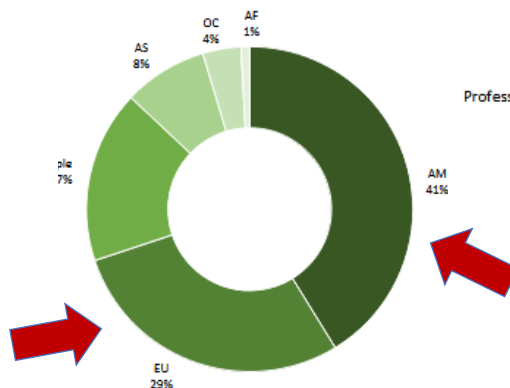
Un contesto in evoluzione | Il rapporto del Clusit 1° sem 2024



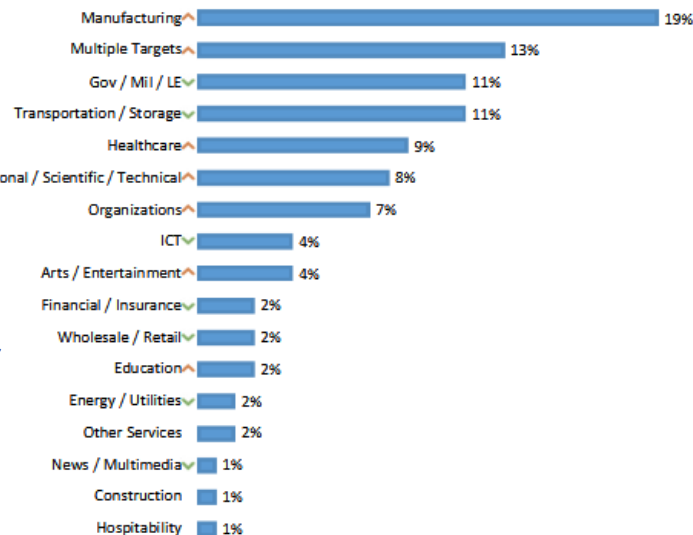
Distribuzione delle vittime H1 2024



Geografia delle vittime H1 2024



Vittime in Italia H1 2024



Valutare il rischio tenendo conto della «value chain»



99%

PMI in Italia



48,5

età media oggi in Italia

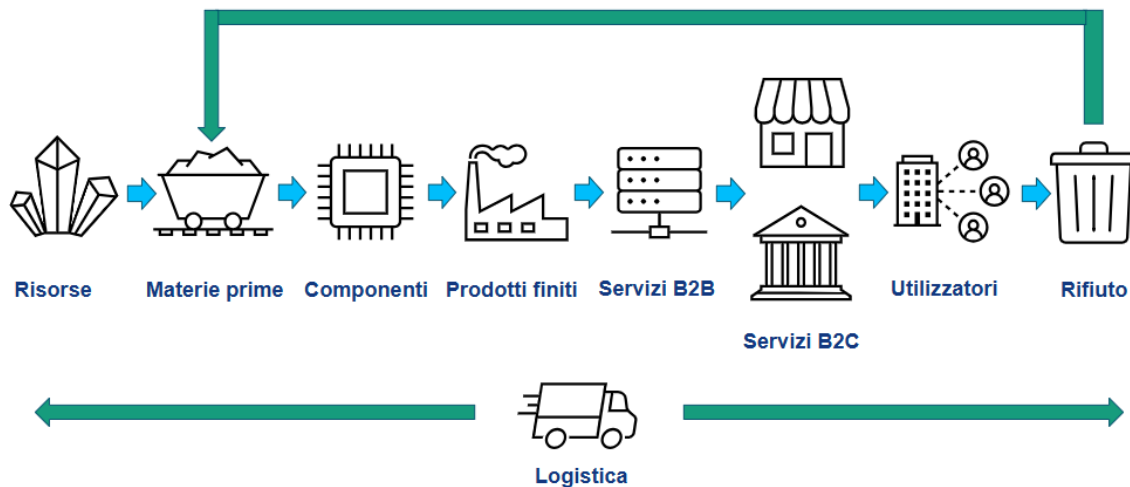
52,5

età media nel 2050 in Italia

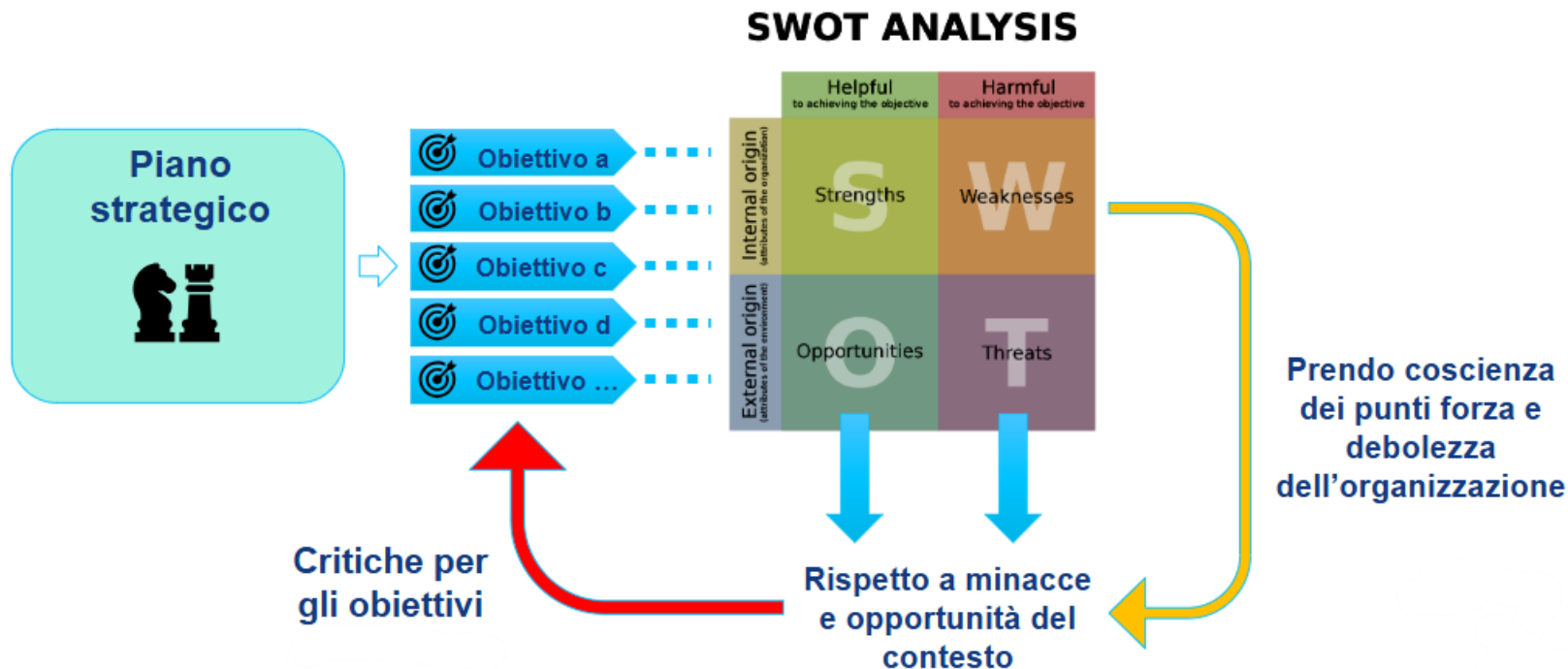


100k

fabbisogno di professional IT

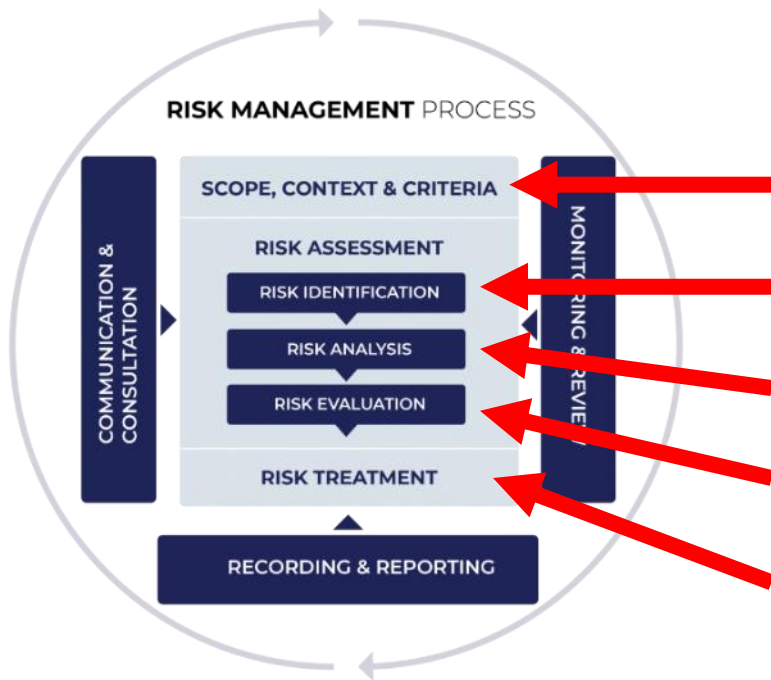


Valutare il rischio guardando agli «obiettivi strategici» e non solo agli aspetti tecnici



Siamo tutti Risk Manager e non lo sappiamo? L'approccio ISO 31000...

Un esempio: cosa fanno gli operatori sanitari?



Fanno domande
Visitano il paziente

Anamnesi

Storia clinica di un soggetto in esame, raccolta dal medico direttamente o indirettamente come elemento fondamentale per la formulazione della diagnosi; comprende le notizie sui precedenti ereditari e sullo stato di salute dei familiari (*a. familiare e personale*), sullo svolgimento dei vari avvenimenti fisiologici, come la dentizione, la crescita, la deambulazione, le abitudini di vita, ecc. (*a. fisiologica*), e la storia delle malattie sofferte dal paziente (*a. patologica*).

Elaborano le info raccolte

Quadro clinico

È l'insieme delle manifestazioni, segni e sintomi, con le quali una malattia si presenta all'osservazione del medico. In questo senso contribuisce in maniera decisiva al raggiungimento della diagnosi di una malattia.

Valutano le varie ipotesi

Diagnosi

La diagnosi è quel processo di analisi che permette di determinare da quale patologia sia affetto un paziente analizzandone sintomi, segni e storia clinica.

Elaborano una soluzione

Prognosi

La prognosi è un giudizio di previsione sul probabile andamento della malattia. Viene formulata una volta fatta la diagnosi, considerando l'usuale tempistica di guarigione, le condizioni del malato, le possibilità terapeutiche e possibili complicazioni o le condizioni ambientali.

Definiscono come intervenire

Terapia

Studio e attuazione concreta dei mezzi e dei metodi per combattere la malattia

Dato

E' la materia prima grezza: numeri, simboli, caratteri, parole, codici.
Singolarmente **non hanno alcun valore** (es. «Federico» è un dato)

Informazione

Risultato dell'elaborazione, contestualizzazione ed elaborazione di uno o più dati. L'informazione è un **asset intangibile aziendale** (es. un brevetto)

Sicurezza delle informazioni?

Significa rendere sicure **le informazioni** (asset intangibili) **e gli asset fisici** che li contengono (asset tangibili).



Sicurezza delle informazioni: il rischio cyber non è soltanto cyber!

Informazione



Dove è custodita?



Dove sono custoditi?



Dove è custodito?



Le contromisure
ISO 27001 – Annex A

- ☐ 37 contromisure **organizzative**
- ☐ 8 contromisure sulle **persone**
- ☐ 14 contromisure **fisiche**
- ☐ 34 contromisure **tecnologiche**



(C) Riservatezza - Confidentiality

Garantire la riservatezza (privacy) dei dati creati, custoditi, trasmessi e diffusi evitandone l'accesso a utenti non autorizzati



(I) Integrità - Integrity

Garantire la protezione del dato da qualsiasi tentativo di manomissione dello stesso, prevenendo alterazione o cancellazione non autorizzata.



(A) Disponibilità - Availability

Garantire la continuità alla fruizione e all'accesso di dati e servizi, impedendo interruzioni nell'erogazione di servizi hardware e software

LA REPUTAZIONE!

**Il problema non è risolvere l'incidente
e cosa rimane dopo averlo risolto.**



It takes 20 years to build a
reputation and five minutes to ruin
it. If you think about that, you'll do
things differently.

— *Warren Buffett* —

GRAZIE! 😊

federico.lucia@fortaris.com

