Laboratorio sugli strumenti di valutazione del rischio cyber

Massimo Battaglioni
Università Politecnica delle Marche
Dipartimento di Ingegneria dell'Informazione
massimo.battaglioni@unimc.it

A.A. 2023/2024

Metodo HTMA

- Il metodo **HTMA** ("How To Measure Anything in cybersecurity risk" [1]) è un metodo *quantitativo* di valutazione del rischio basato su Simulazioni Monte Carlo

- HTMA si compone di quattro passaggi:

1. Definizione *della lista degli eventi* (minacce) cyber di cui si vuole valutare il rischio
2. Stima della *probabilità di accadimento* e dell'*impatto* di ciascun evento
3. Generazione degli scenari attraverso la *simulazione Monte Carlo*
4. Interpretazione dei *risultati*

[1] D. Hubbard e R. Seiersen, How to Measure Anything in Cybersecurity Risk, Wiley, 2016

Metodo FAIR

- Il metodo **FAIR** ("Factor Analysis of Information Risk" [2]) è un metodo *quantitativo* di valutazione del rischio basato su un'Ontologia del Rischio e su Simulazioni Monte Carlo

- FAIR si compone di quattro passaggi:

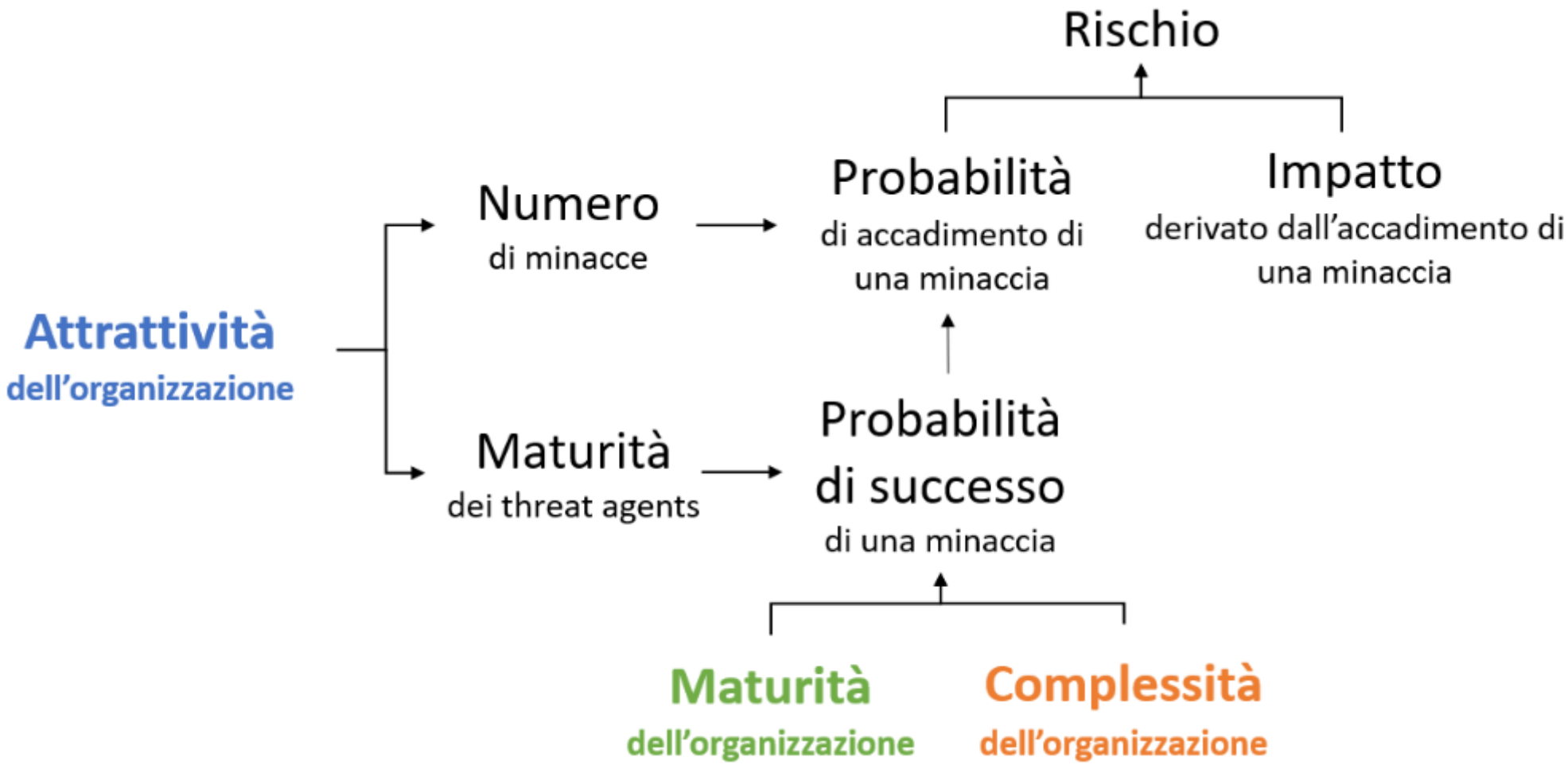
1. Definizione *dello scenario* sotto esame e decomposizione in sotto-scenari
2. Stima dei *parametri* per ogni sotto-scenario
3. Generazione dei framework attraverso la *simulazione Monte Carlo*
4. Interpretazione dei *risultati*

[2] J. Freund and J. Jones, Measuring and Managing Information Risk: A FAIR Approach. Butterworth-Heinemann, 2014.

HTMA – FAIR – MIX METHOD

https://cegisa.shinyapps.io/qrisk_mix/

MAGIC


Rischio
Probabilità
di accadimento di una minaccia
Impatto
derivato dall'accadimento di una minaccia
Numero
di minacce
Attrattività
dell'organizzazione
Maturità
dei threat agents
Probabilità di successo
di una minaccia
Maturità
dell'organizzazione
Complessità
dell'organizzazione

MAGIC-HTMA

https://github.com/secomms/cyber-risk-assessment

https://secomms.shinyapps.io/cybeRAMA/