UNIVERSITÀ POLITECNICA DELLE MARCHE

DII Dipartimento di Ingegneria dell'Informazione

unimc

STRUMENTI DI VALUTAZIONE DEL RISCHIO IN CYBERSECURITY

Pierre ABI SAFI

Ingegnere Civile Edile

EdiliziaLebanon – consulting and construction

https://edilizialb.business.site/

Cel. +39.780850759

Martedì 19 Luglio 2022

Corso di Perfezionamento in Cybersecurity, Cyber Risk and Data Protection

CYBERSECURITY OBBIETTIVI

GARANTIRE

RISERVATEZZA
INTEGRITÀ
DISPONIBILITÀ
RESILIANZA

DEL SISTEMA

A fine di Garantire tali obbiettivi di cybersecurity é necessario individuare ed analizzare le

1. **Minacce**
2. **Vulnerabilità**
3. **Rischi**

Che un sistema informatico andrebbe ad affrontare

Analisi e Gestione del rischio Cyber

L’ *Analisi del rischio* parte dall'identificazione degli Asset da proteggere;

- Si valutano quindi le possibili Minacce, la loro **Probabilità** di occorrenza e il relativo **Impatto** inteso come danno potenziale (gravità).
- Il rischio viene stimato in funzione a questi variabili dalla formula

In base alla Valutazione del Rischio si decide se, come e quali contromisure di sicurezza adottare (piano di rischio).

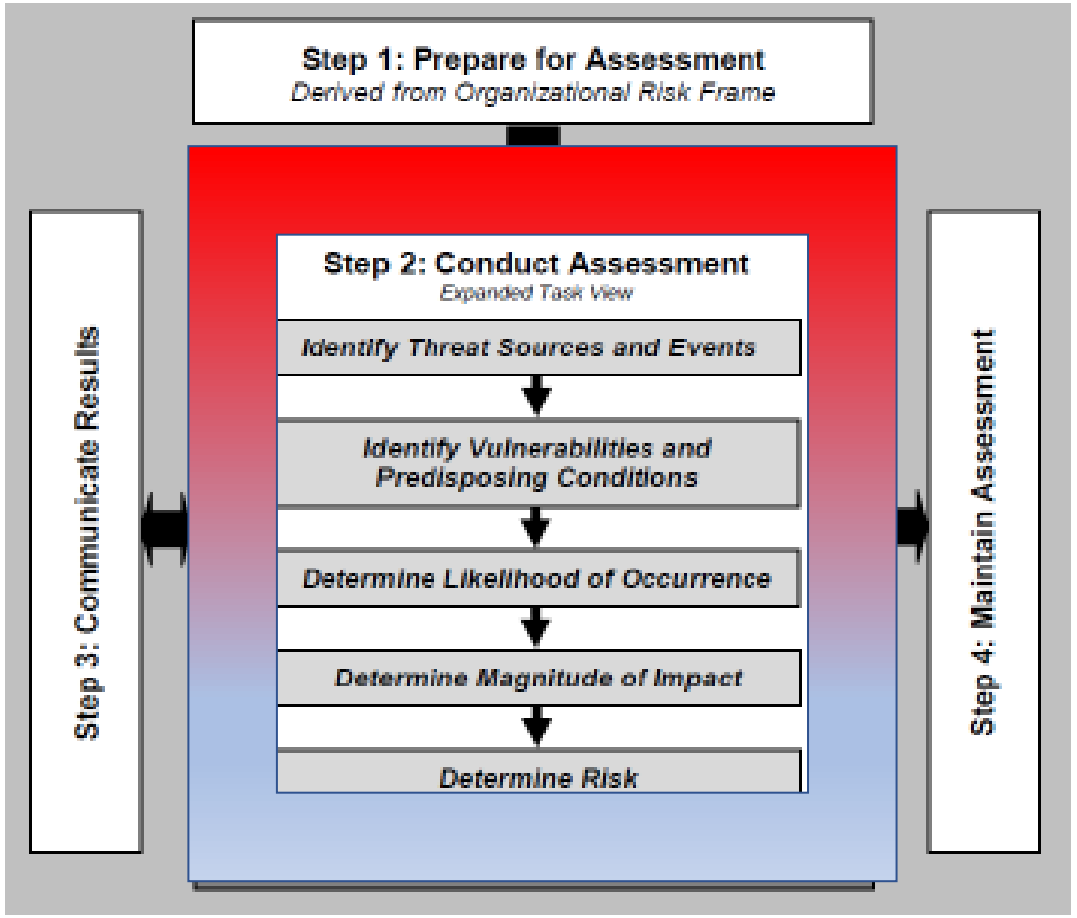
CYBERISK ASSESSMENT PROCEDURE– (Procedura di Valutazione del Rischio Cyber)

Corso di Perfezionamento in Cybersecurity, Cyber Risk and Data Protection

Risk Assessment Procedure

NIST SP 800-30r1, Guide for Conducting Risk Assessments

1. **Analizzare le minacce**
2. **Analizzare le vulnerabilità e i fattori predisponenti**
3. **Determinare la probabilità di accadimento**
4. **Determinare l'entità dell'impatto**
5. **DETERMINARE IL RISCHIO**



Strumenti per detrminare il rischio in cybersecurity

Strumenti di valutazione del Rischio in cybersecurity

- Le norme e gli standard forniscono delle indicazioni su come, in generale, valutare i rischi, ma non forniscono degli strumenti per farlo

- Molti strumenti sono stati sviluppati sia da Enti Nazionali e internazionali, sia nella letteratura scientifica
- Generalmente questi strumenti possono essere divisi in 2 gruppi principali
- 1. QUALITATIVI
- 2. QUANTITATIVI

Cyberisk Assessment Tools - Metodo Qualitativo

La valutazione qualitativa utilizza tipicamente una serie di metodi, principi o regole basati su categorie o livelli non numerici per la valutazione del rischio date da esperti cyber

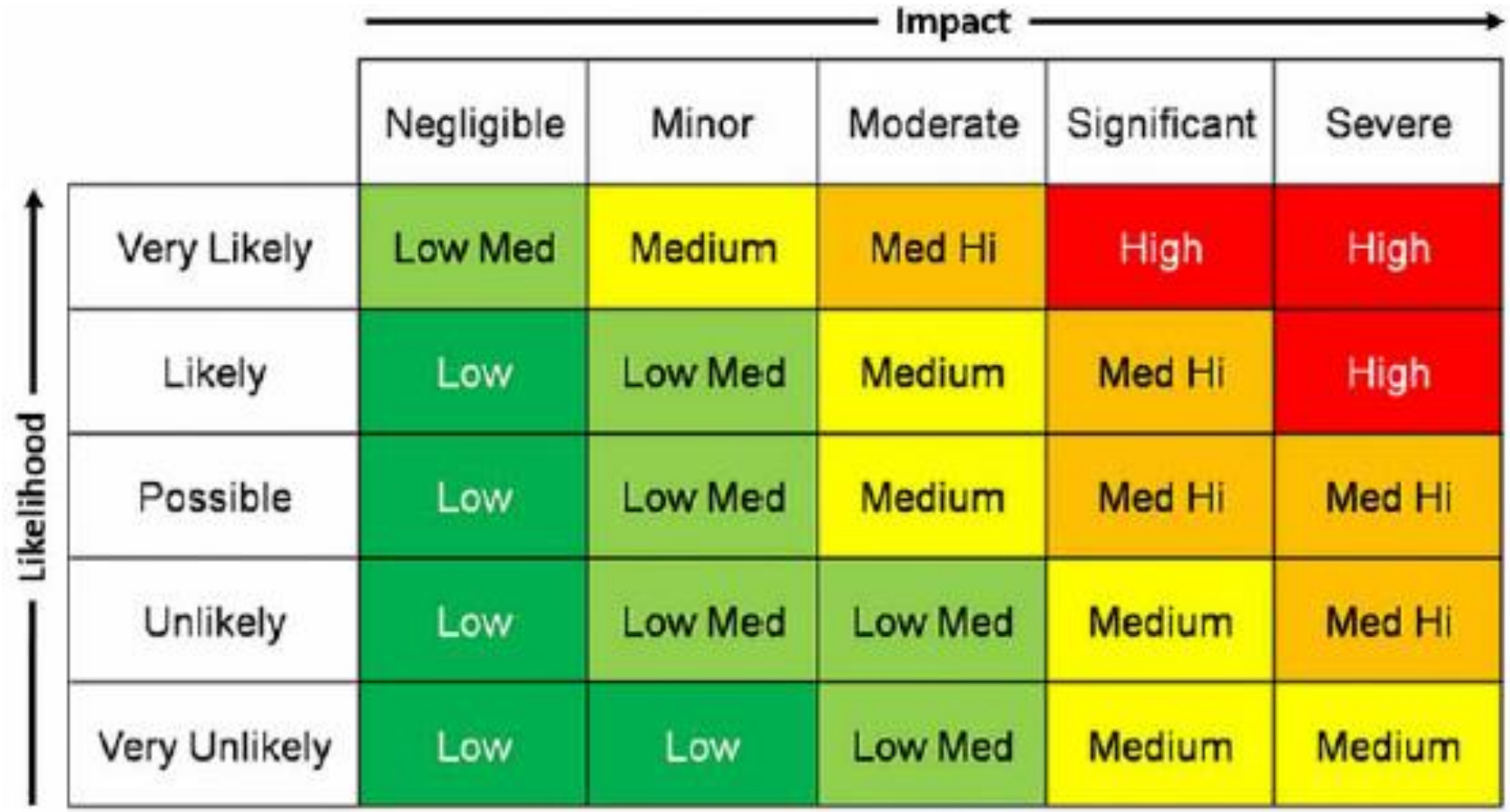
PRO

- Efficienti in termini di tempo e costi, poiché non richiedono la stima di valori esatti
- Possono essere utilizzati per identificare facilmente le possibili aree di miglioramento

CONTRO

- Esperti diversi potrebbero produrre risultati significativamente diversi
- Riprodurre o confrontare i risultati può essere difficile, spesso impossibile

Metodo Qualitativo - Matrice del rischio



Esempio di matrice del rischio (adottata dalla Federal Aviation Administration del Dipartimento dei trasporti degli Stati Uniti)

Impatto (ascisse) ; Probabilità (ordinate) tutte due a valutazione

Cyberisk Assessment Tools - Metodo Quantitativo

La valutazione quantitativa utilizza tipicamente una serie di metodi, principi o regole per la valutazione del rischio basati sull'uso di numeri

PRO

- I risultati della valutazione quantitativa sono rigorosi, ripetibili e riproducibili
- La stima delle probabilità e degli impatti degli eventi può essere confrontata in modo diretto e oggettivo

CONTRO

- La stima delle probabilità e degli impatti è molto impegnativa e i risultati potrebbero non essere sempre chiari
- I benefici possono non essere bilanciati dai costi e dalla possibilità di disporre di strumenti per effettuare le necessarie valutazioni

Metodo Quantitativo 1: HTMA - Procedura

Il metodo HTMA ("**How To Measure Anything** in cybersecurity risk") è un metodo quantitativo di valutazione del rischio basato sulla Simulazione 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 accadmento e dell'impatto di ciascun evento**

Event	Probability	LB 90% CI	UB 90% CI
ransomware	0.50	€10,000	€300,000
Malware	0.20	€20,000	€500,000
pishing	0.10	€20,000	€100,000

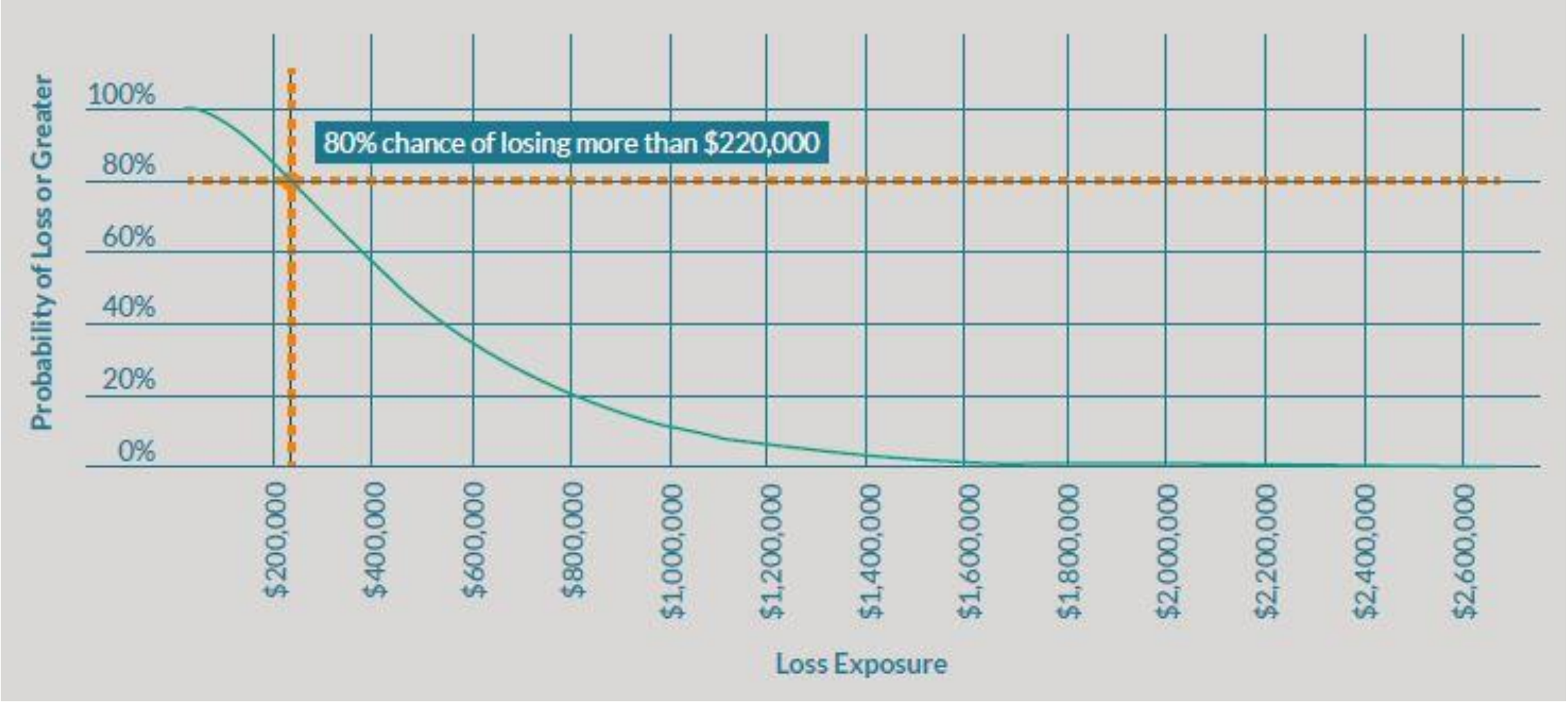
3. **Generazione degli scenari attraverso la simulazione Monte Carlo**
4. **Interpretazione dei risultati**

SIMULAZIONE MONTE CARLO

Un algoritmo che utilizza una campionatura casuale ripetuta un elevato numero di volte per ottenere la probabilità del verificarsi di un intervallo di risultati

Metodo Quantitativo 1: HTMA – Forma dei Risultati

Output HTMA : Curve di Perdita – Loss Exceedance Curve (LEC)



Metodo Quantitativo 2: FAIR - Procedura

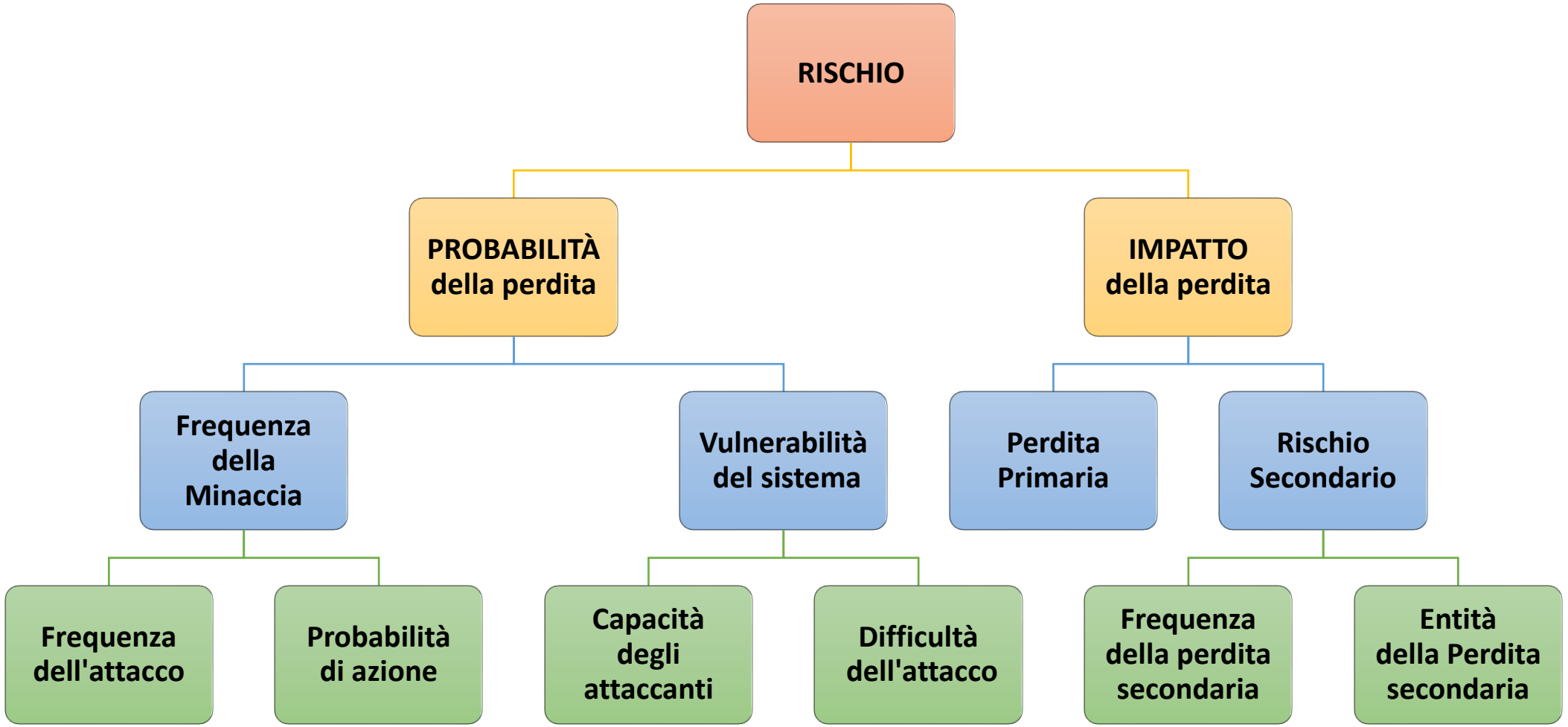
Il metodo FAIR (Factor Analysis of Information Risk) è un metodo quantitativo di valutazione del rischio basato su un'Ontologia del Rischio e su Simulazioni Monte Carlo

FAIR si compone in 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

Metodo Quantitativo 2: FAIR – SCHEMA PERT

La Stima dei parametri per ogni sotto-scenario fondata su un'ontologia del rischio



Metodo Quantitativo 2: FAIR – Forma dei Risultati

- I risultati sono solitamente presentati tramite:
- Grafici a dispersione: riportano frequenza e entità della perdita primaria e secondaria per ciascuno scenario generato con la simulazione Monte Carlo
- Tabelle riassuntive: riportano i valori minimo, medio, più verosimile e massimo ottenuti con la simulazione Monte Carlo per ciascuna delle variabili di interesse
- Percentili: rappresentano il 10° e il 90° percentile della perdita totale

malevola - computer Central - malati aids - canacellazione - loss data

	Minimum	Average	Most Likely	Maximum
Primary Loss Events/Year	0.051	2.28	0.80	19.14
Primary Loss Magnitude	€28,313	€39,141	€38,762	€52,314
Secondary Loss Events/Year	0.05	2.23	0.78	18.65
Secondary Loss Magnitude	€30,352	€589,809	€359,102	€2,727,110
Total Loss Exposure	€12,302	€1,386,490	€375,178	€13,149,063

Summary Table

€132,715
10% percentile of Total Loss Exposure

€3,191,020
90% percentile of Total Loss Exposure

Metodo Quantitativo 3: MAGIC - Procedura

MAGIC è un metodo quantitativo che mira a risolvere la stima della Probabilità di accadimento degli eventi in modo il **più oggettivo possible**

Si valutano quindi con cura i tre fattori principali : Attrattività, Maturità, Complessità e si procede come segue

Metodo Quantitativo 3: MAGIC - Forma dei Risultati -Indici

I risultati degli tre fattori principali valutati da 0 a 10 per : Attrattività, Maturità, Complessità

Valutazione Complessità

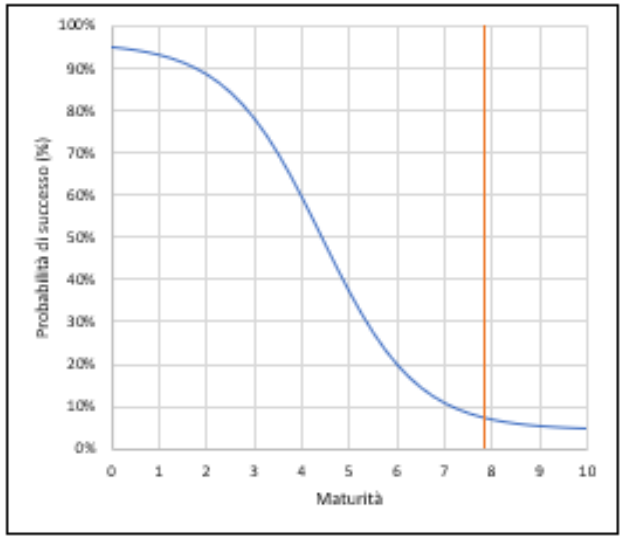
Profilo complessità *(per categoria)*	Livello di complessità	Complessità pesata	Num. quesiti	Peso %
Reti e infrastruttura	***Moderata***	***5.07***	11	37.93%
Tecnologie su reti IP	***Moderata***	**3.75**	4	13.79%
Applicazioni	***Significativa***	**8.30**	5	17.24%
Servizi online	***Moderata***	**4.17**	3	10.34%
Reparto IT	***Minima***	**0.47**	6	20.69%
Complessità media	***Bassa***	***4.35***	**tot**	**tot**
Complessità media pesata	***Bassa***	***4.40***	**29**	**100.00%**

Attrattività	**Molto Alta**
Peso attrattività	1

Indice di maturità medio	**6.47**

Probabilità di successo di un attacco	7%

Probabilità di successo di un attacco pesata	7%



UNIVERSITÀ POLITECNICA DELLE MARCHE

DII
Dipartimento di Ingegneria dell'Informazione

unimc

STRUMENTI DI VALUTAZIONE DEL RISCHIO IN CYBERSECURITY

FINE

GRAZIE

Martedì 19 Luglio 2022

Corso di Perfezionamento in Cybersecurity, Cyber Risk and Data Protection