Valutazione del rischio cyber

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

A.A. 2023/2024

Analisi del rischio

- Il rischio è una combinazione di probabilità e di gravità:

$$R = P \text{ x } \mathrm{I}$$

[€] [€]

$0 \leq P \leq 1$
adimensionale

Analisi del rischio – Due casi estremi

$$R = ??$$

Analisi del rischio

- Il rischio è una combinazione di probabilità e di gravità:

$$R = P \times Vu \times Val$$

P = Probabilità dell'attacco

Vu = Vulnerabilità all'attacco

Val = Valore del danno provocato nel caso in cui l'attacco abbia successo

Stima del rischio

- La stima del rischio è intrinsecamente difficile a causa della sua imprevedibilità.

Stima del rischio

- La stima del rischio è intrinsecamente difficile a causa della sua imprevedibilità.

- Nei metodi di valutazione del rischio più comuni, vengono stimate le probabilità di accadimento degli eventi sulla base di uno storico, insieme alle possibili conseguenze, ma ciò rende le valutazioni del rischio ed i relativi risultati soggetti ad errori.

Stima del rischio

- La stima del rischio è intrinsecamente difficile a causa della sua imprevedibilità.
- Nei metodi di valutazione del rischio più comuni, vengono stimate le probabilità di accadimento degli eventi sulla base di uno storico, insieme alle possibili conseguenze, ma ciò rende le valutazioni del rischio ed i relativi risultati soggetti ad errori.
- Il rischio e i fattori che vi contribuiscono possono essere valutati in vari modi: *quantitativamente*, *qualitativamente* o *semi-quantitativamente*.

Stima del rischio

- La stima del rischio è intrinsecamente difficile a causa della sua imprevedibilità.
- Nei metodi di valutazione del rischio più comuni, vengono stimate le probabilità di accadimento degli eventi sulla base di uno storico, insieme alle possibili conseguenze, ma ciò rende le valutazioni del rischio ed i relativi risultati soggetti ad errori.
- Il rischio e i fattori che vi contribuiscono possono essere valutati in vari modi: *quantitativamente*, *qualitativamente* o *semi-quantitativamente*.
- Ciascun approccio di valutazione del rischio presenta vantaggi e svantaggi.

Metodi QUALITATIVI

- La *valutazione qualitativa* utilizza tipicamente una serie di metodi, principi o regole basati su categorie o livelli non numerici per la valutazione del rischio

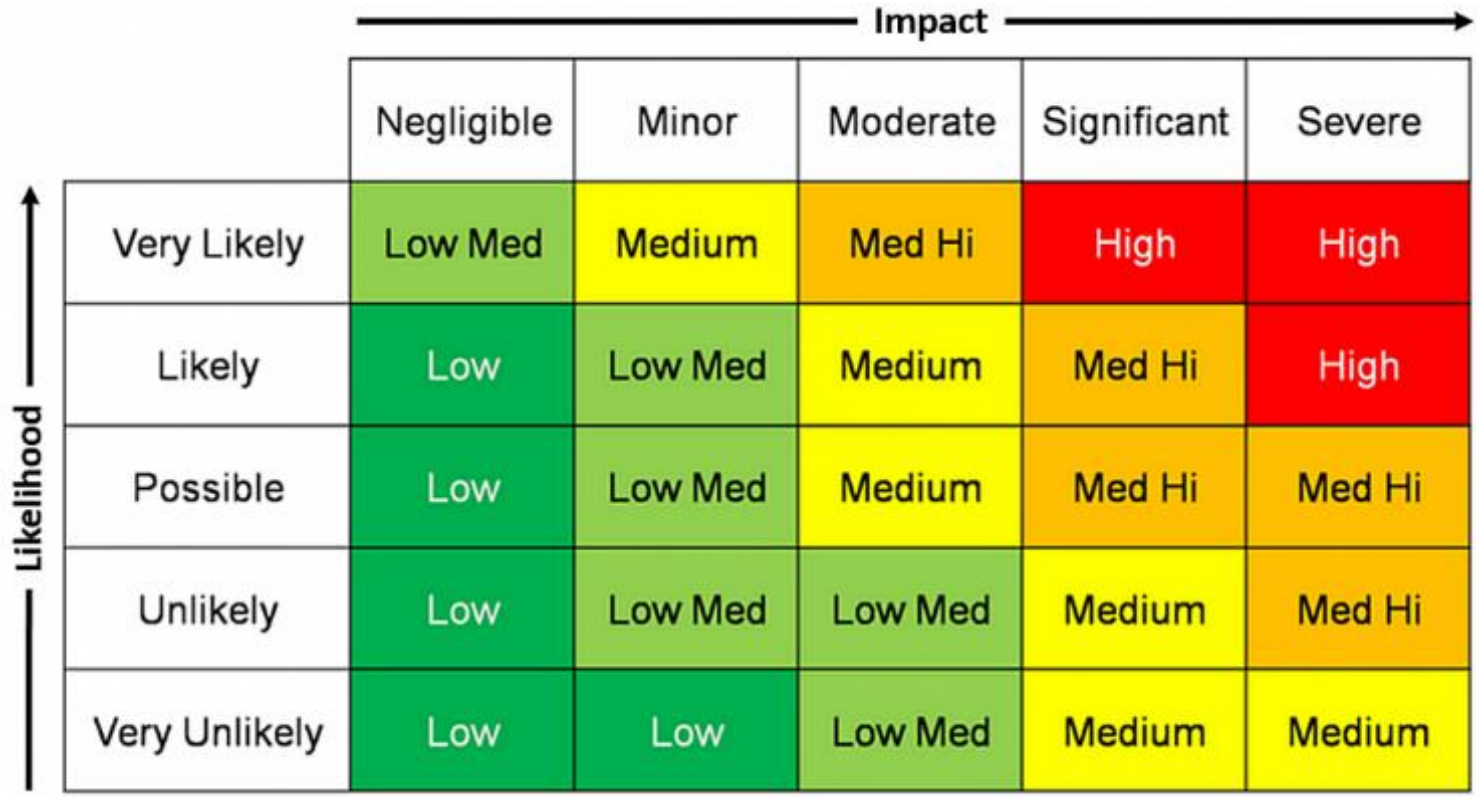
PRO

- 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
- Come fare un'analisi accurata costi benefici?

Matrici di rischio



Metodi QUANTITATIVI

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

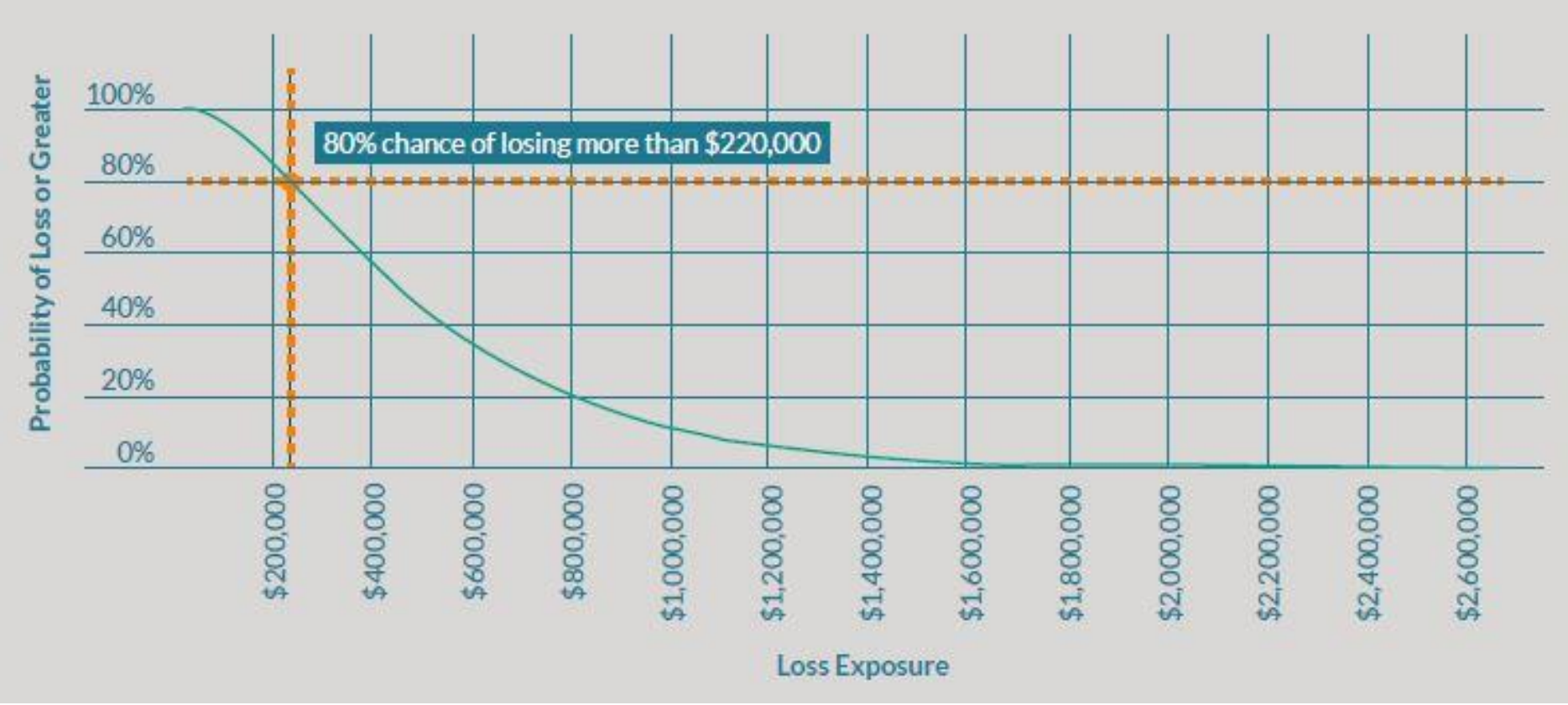
PRO

- 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

Curve di perdita



Metodi SEMI - QUANTITATIVI

- La *valutazione semi-quantitativa* impiega tipicamente una serie di metodi, principi o regole per la valutazione del rischio, utilizzando intervalli, scale o numeri rappresentativi.

PRO

- Si può passare dalla rappresentazione quantitativa a quella qualitativa (ereditando i PRO dei metodi qualitativi)
- Tramite la rappresentazione quantitativa, i confronti numerici sono possibili

CONTRO

- La combinazione e l'interpretazione dei risultati può essere difficile, a causa delle diverse scale di valutazione

Valutazione quantitativa: HTMA

- Il metodo HTMA ("How To Measure Anything in cybersecurity risk" [1]) si compone di quattro passaggi:

1. definizione della lista degli eventi cyber di cui si vuole valutare il rischio;
2. stima della probabilità di occorrenza 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.

Valutazione quantitativa: HTMA

1. **Definizione della lista degli eventi cyber di cui si vuole valutare il rischio.**

   - Il rischio è definito come “uno stato di incertezza in cui alcune delle possibilità comportano una perdita, una catastrofe o un altro esito indesiderato”.

   - Nella lista devono essere elencati degli eventi che comportano un rischio cyber.

   - Il numero e la natura degli eventi da elencare sono a discrezione di chi sta conducendo l’analisi: si possono considerare i rischi associati a una singola vulnerabilità, a un sistema, a un’unità di business o all’intera organizzazione.

Valutazione quantitativa: HTMA

2. Stima della probabilità di occorrenza e dell'impatto di ciascun evento.

Per ogni evento elencato nella lista, gli esperti di cybersecurity dell'organizzazione devono stimare:

Valutazione quantitativa: HTMA

2. Stima della probabilità di occorrenza e dell'impatto di ciascun evento.

Per ogni evento elencato nella lista, gli esperti di cybersecurity dell'organizzazione devono stimare:

- La probabilità di occorrenza (*likelihood*): è la probabilità che l'evento si verifichi in un intervallo temporale dato. Ad ogni evento si associa una probabilità compresa tra 0 e 1.

Valutazione quantitativa: HTMA

2. Stima della probabilità di occorrenza e dell'impatto di ciascun evento.

Per ogni evento elencato nella lista, gli esperti di cybersecurity dell'organizzazione devono stimare:

- La probabilità di occorrenza (*likelihood*): è la probabilità che l'evento si verifichi in un intervallo temporale dato. Ad ogni evento si associa una probabilità compresa tra 0 e 1.

- L'impatto ad esso associato nel caso in cui l'evento si verifichi, in termini di perdita monetaria (*impact*); è la perdita monetaria associata al verificarsi dell'evento in un intervallo temporale dato. Si stima attraverso un intervallo di confidenza (CI), cioè un intervallo di valori plausibili per quel parametro, del 90%, individuato da un limite inferiore (LB) e un limite superiore (UB).

Valutazione quantitativa: HTMA

2. Stima della probabilità di occorrenza e dell'impatto di ciascun evento.

Minaccia	Probabilità	LB	UB
e_1	p_1	LB_1	UB_1
e_2	p_2	LB_2	UB_2
…	…	…	…
e_N	p_N	LB_N	UB_N

Valutazione quantitativa: HTMA

3. Generazione degli scenari attraverso la simulazione Monte Carlo.

Gli eventi elencati nella lista, con le rispettive probabilità di occorrenza e i rispettivi impatti, vengono usati come input per la simulazione Monte Carlo.

Valutazione quantitativa: HTMA

3. Generazione degli scenari attraverso la simulazione Monte Carlo.

Gli eventi elencati nella lista, con le rispettive probabilità di occorrenza e i rispettivi impatti, vengono usati come input per la simulazione Monte Carlo.

Effettuare una simulazione Monte Carlo significa studiare l'andamento di una variabile aleatoria di interesse simulandone un campionamento casuale attraverso la generazione di un numero elevato di scenari, in cui di volta in volta la variabile viene calcolata a partire da variabili note.

Simulazione Monte Carlo

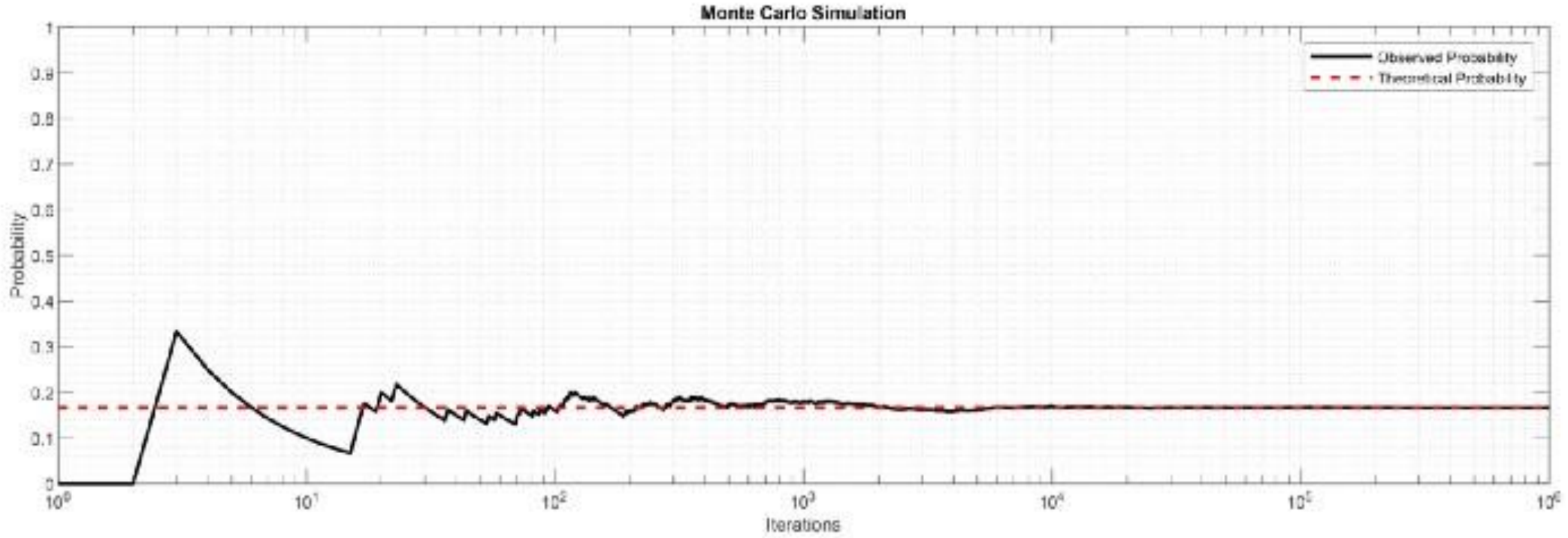
- Qual è la probabilità che, lanciando un dado, io ottenga 4?

$$\text{probabilità} = \frac{\text{casi favorevoli}}{\text{casi possibili}} \quad \Rightarrow \quad p = \frac{1}{6} \cong 0.17$$

- Quindi, lanciando un dado 6 volte, sicuramente 4 uscirà una volta?

- La probabilità che si verifichi un evento coincide solo con il valore teorico quando l'esperimento viene eseguito infinite volte

Simulazione Monte Carlo



Probabilità **teorica**

Valutazione quantitativa: HTMA

3. Generazione degli scenari attraverso la simulazione Monte Carlo.

Gli eventi elencati nella lista, con le rispettive probabilità di occorrenza e i rispettivi impatti, vengono usati come input per la simulazione Monte Carlo.

Effettuare una simulazione Monte Carlo significa studiare l'andamento di una variabile aleatoria di interesse simulandone un campionamento casuale attraverso la generazione di un numero elevato di scenari, in cui di volta in volta la variabile viene calcolata a partire da variabili note.

La variabile aleatoria di interesse, in questo caso, è il *rischio totale annuale* derivante dagli eventi cyber elencati nella lista, espresso come perdita monetaria. Il valore del rischio totale annuale corrisponde alla somma degli impatti degli eventi che si sono verificati, e dipende quindi, in ogni scenario, da quali eventi si verificano e dall'entità della perdita ad essi associata.

Valutazione quantitativa: HTMA

3. Generazione degli scenari attraverso la simulazione Monte Carlo.

Pertanto, all'interno di un singolo scenario:

- Va simulata l'occorrenza di ciascun evento (si è verificato o non si è verificato) compatibilmente con la sua probabilità;

Valutazione quantitativa: HTMA

3. Generazione degli scenari attraverso la simulazione Monte Carlo.

Pertanto, all'interno di un singolo scenario:

- Va simulata l'occorrenza di ciascun evento (si è verificato o non si è verificato) compatibilmente con la sua probabilità;
- Per gli eventi che non si sono verificati il rispettivo impatto viene posto pari a 0, mentre per ogni evento che si è verificato va generato l'impatto ad esso associato, compatibilmente con il range individuato dal suo CI del 90%;

Valutazione quantitativa: HTMA

3. Generazione degli scenari attraverso la simulazione Monte Carlo.

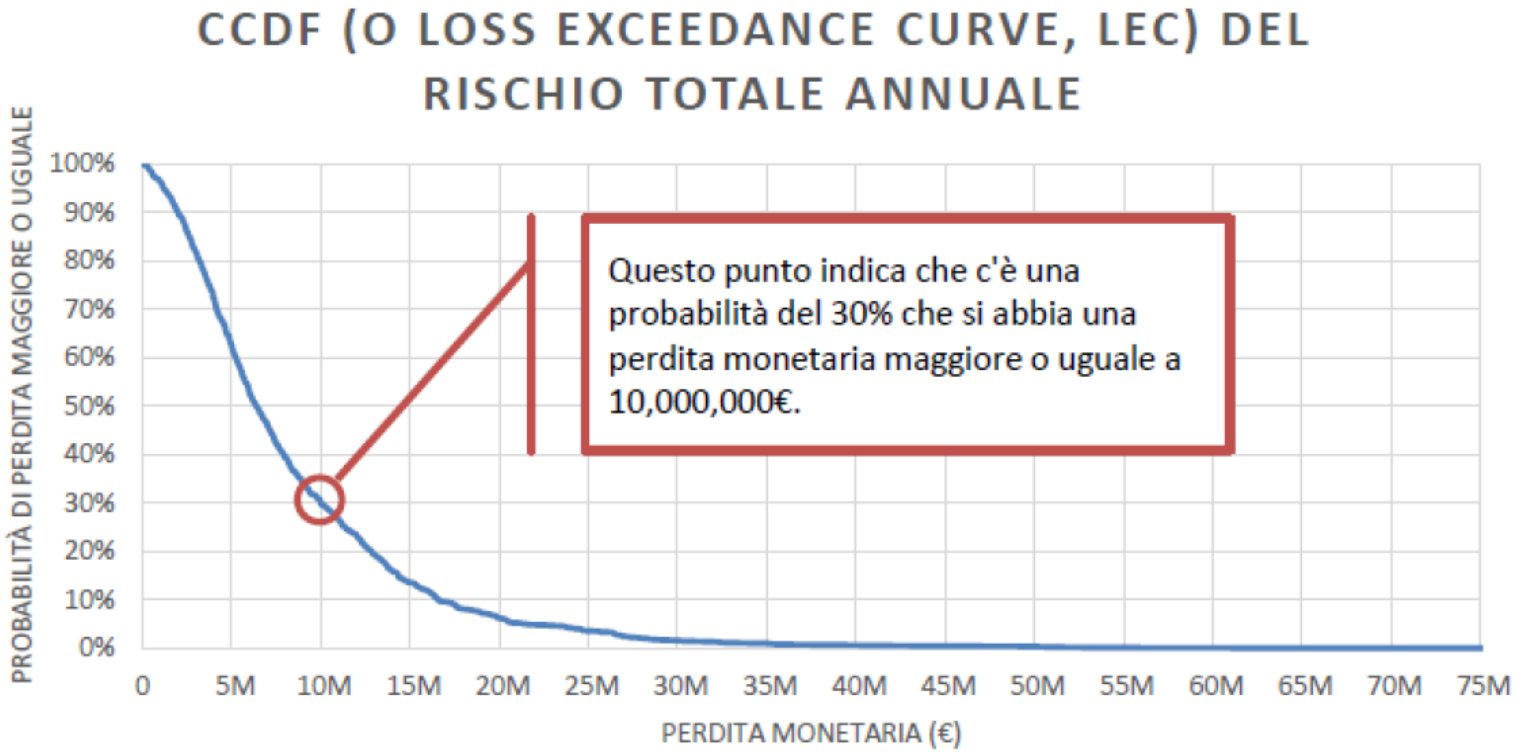
Pertanto, all'interno di un singolo scenario:

- Va simulata l'occorrenza di ciascun evento (si è verificato o non si è verificato) compatibilmente con la sua probabilità;
- Per gli eventi che non si sono verificati il rispettivo impatto viene posto pari a 0, mentre per ogni evento che si è verificato va generato l'impatto ad esso associato, compatibilmente con il range individuato dal suo CI del 90%;
- Gli impatti generati per tutti gli eventi che si sono verificati vanno sommati, in modo da ottenere l'impatto totale che corrisponde al rischio totale annuale.

Valutazione quantitativa: HTMA

4. Interpretazione dei risultati.

I risultati ottenuti con la simulazione Monte Carlo vengono usati per costruire la Loss Exceedance Curve, o LEC, che corrisponde alla rappresentazione grafica della Complementary Cumulative Distribution Function (CCDF) del rischio totale annuale (o ALE).



HTMA: esempio di applicazione

- Si considerano 50 eventi, caratterizzati dai parametri indicati in Tabella. In particolare, per ogni evento, viene indicata la probabilità di occorrenza e il limite inferiore e superiore dell'intervallo di confidenza relativo all'impatto dell'evento.

-	Probabilità	LB CI-90% (€)	UB CI-90% (€)
Event 1	0.02	40,000	200,000
Event 2	0.05	500,000	2,000,000
Event 3	0.10	400,000	2,500,000
Event 4	0.15	100,000	5,000,000
Event 5	0.20	25,000	500,000
Event 6	0.12	200,000	5,000,000
Event 7	0.08	20,000	750,000
Event 8	0.11	1,000,000	3,000,000
Event 9	0.40	200,000	2,000,000
Event 10	0.02	1,000,000	10,000,000
Event 11	0.25	40,000	200,000
Event 12	0.02	500,000	2,000,000
Event 13	0.09	400,000	10,000,000
Event 14	0.04	5,000,000	25,000,000
Event 15	0.05	500,000	5,000,000
Event 16	0.06	200,000	5,000,000
Event 17	0.12	200,000	2,000,000
Event 18	0.02	1,000,000	3,000,000
Event 19	0.03	200,000	2,000,000
Event 20	0.11	25,000	500,000
Event 21	0.23	200,000	5,000,000
Event 22	0.34	20,000	750,000
Event 23	0.21	1,000,000	3,000,000
Event 24	0.13	40,000	200,000
Event 25	0.02	500,000	2,000,000
Event 26	0.07	400,000	10,000,000
Event 27	0.05	100,000	5,000,000
Event 28	0.02	25,000	500,000
Event 29	0.45	200,000	5,000,000
Event 30	0.35	20,000	750,000
Event 31	0.09	1,000,000	3,000,000
Event 32	0.04	200,000	2,000,000
Event 33	0.05	1,000,000	10,000,000
Event 34	0.06	40,000	200,000
Event 35	0.12	500,000	2,000,000
Event 36	0.02	400,000	10,000,000
Event 37	0.03	100,000	5,000,000
Event 38	0.15	3,000,000	15,000,000
Event 39	0.23	200,000	5,000,000
Event 40	0.34	20,000	750,000
Event 41	0.21	1,000,000	3,000,000
Event 42	0.02	200,000	2,000,000
Event 43	0.03	1,000,000	10,000,000
Event 44	0.11	2,000,000	20,000,000
Event 45	0.23	40,000	500,000
Event 46	0.34	10,000	100,000
Event 47	0.21	30,000	500,000
Event 48	0.13	100,000	1,000,000
Event 49	0.02	2,000,000	5,000,000
Event 50	0.07	1,000,000	20,000,000

HTMA: esempio di applicazione

- Per simulare la frequenza di occorrenza di ciascun evento si procede come segue:

1. Prendere in input le probabilità di ogni evento (p_i);

HTMA: esempio di applicazione

- Per simulare la frequenza di occorrenza di ciascun evento si procede come segue:

1. Prendere in input le probabilità di ogni evento (p_i);

2. Generare un numero random r ∈ [0, 1] da una distribuzione uniforme U(0, 1).

- se $r < p_i$ l'evento si è verificato;
- se $r \geq p_i$ l'evento non si è verificato.

HTMA: esempio di applicazione

- Per simulare la frequenza di occorrenza di ciascun evento si procede come segue:

1. Prendere in input le probabilità di ogni evento (p_i);
2. Generare un numero random $r \in [0, 1]$ da una distribuzione uniforme U(0, 1).

- se $r < p_i$ l'evento si è verificato;
- se $r \geq p_i$ l'evento non si è verificato.

- Per generare un impatto I_i compatibile con il CI al 90% dell'evento e_i si procede come segue:

1. Prendere in input: LB_i e UB_i del CI al 90%;

HTMA: esempio di applicazione

➢ Per simulare la frequenza di occorrenza di ciascun evento si procede come segue:

1. Prendere in input le probabilità di ogni evento (p_i);
2. Generare un numero random r ∈ [0, 1] da una distribuzione uniforme U(0, 1).

- se $r < p_i$ l'evento si è verificato;
- se $r \geq p_i$ l'evento non si è verificato.

➢ Per generare un impatto I_i compatibile con il CI al 90% dell'evento e_i si procede come segue:

1. Prendere in input: LB_i e UB_i del CI al 90%;
2. Associare all'impatto I_i una distribuzione di probabilità log-normale, derivando la relativa media e deviazione standard da LB_i e UB_i in questo modo:

- $\mu = \frac{\ln(UB_i)+\ln(LB_i)}{2}$
- $\sigma = \frac{\ln(UB_i)+\ln(LB_i)}{3.29}$

HTMA: esempio di applicazione

- Per simulare la frequenza di occorrenza di ciascun evento si procede come segue:

1. Prendere in input le probabilità di ogni evento (p_i);
2. Generare un numero random r ∈ [0, 1] da una distribuzione uniforme U(0, 1).

- se $r < p_i$ l'evento si è verificato;
- se $r \geq p_i$ l'evento non si è verificato.

- Per generare un impatto I_i compatibile con il CI al 90% dell'evento e_i si procede come segue:

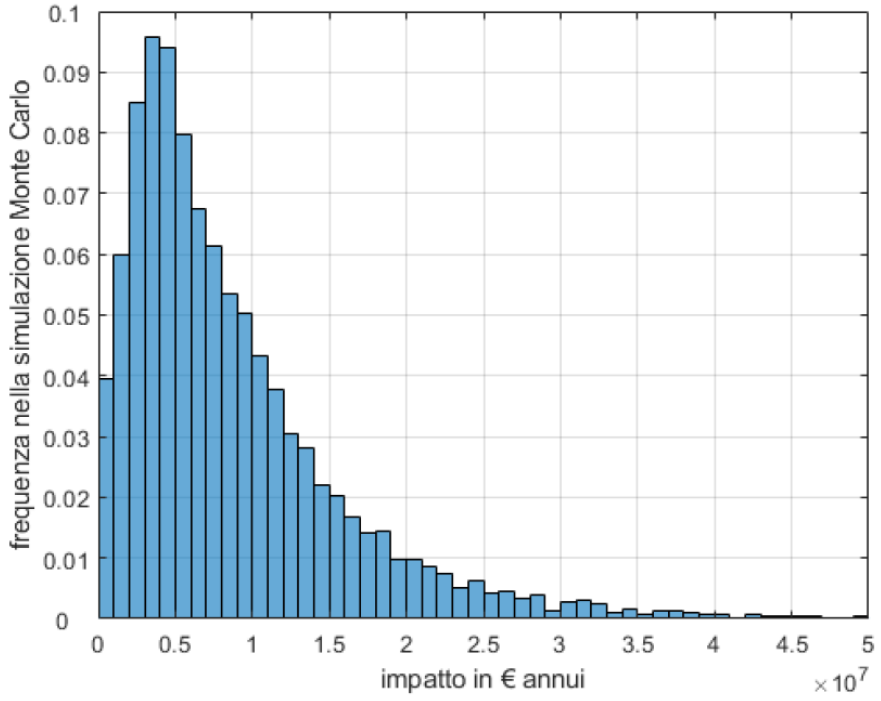
1. Prendere in input: LB_i e UB_i del CI al 90%;
2. Associare all'impatto I_i una distribuzione di probabilità log-normale, derivando la relativa media e deviazione standard da LB_i e UB_i
3. Estrarre un campione random dalla popolazione la cui distribuzione è stata definita al passo 2: questo valore corrisponde all'impatto I_i dell'evento.

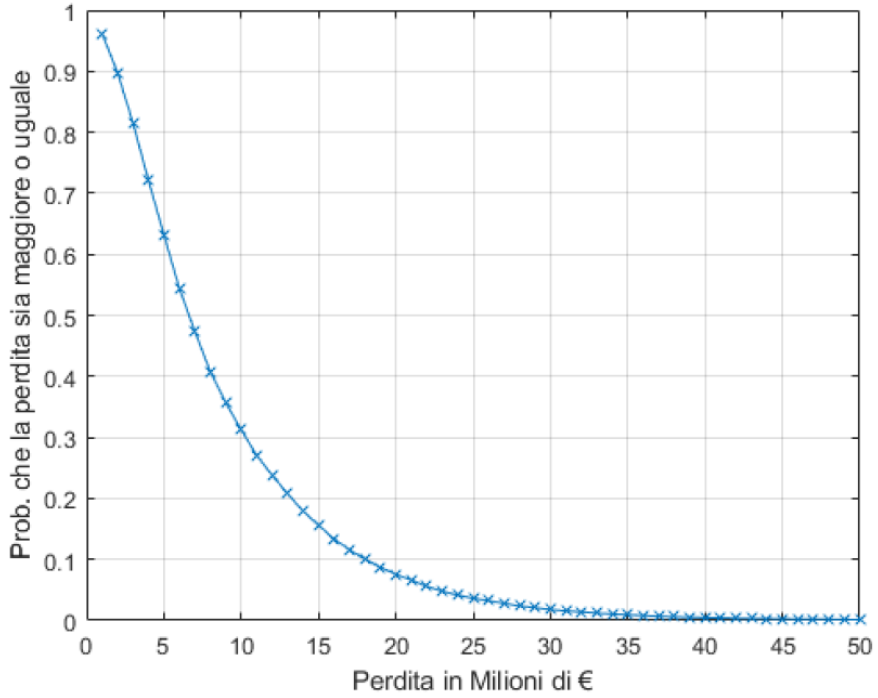
HTMA: esempio di applicazione

- La simulazione Monte Carlo consiste nel ripetere questa procedura un numero elevato di volte, così da poter costruire la distribuzione del rischio totale annuale a partire dai valori assunti da questa variabile in ciascuno scenario generato. Ogni iterazione della simulazione prevede di applicare la procedura sopra descritta a ogni evento della tabella in input.

HTMA: esempio di applicazione

- La simulazione Monte Carlo consiste nel ripetere questa procedura un numero elevato di volte, così da poter costruire la distribuzione del rischio totale annuale a partire dai valori assunti da questa variabile in ciascuno scenario generato. Ogni iterazione della simulazione prevede di applicare la procedura sopra descritta a ogni evento della tabella in input.
- Esempio: Simulazione Monte Carlo con 10,000 iterazioni.





Valutazione quantitativa: FAIR

- Il metodo FAIR [2] si compone di quattro passaggi:

1. definizione dello scenario di cui si vuole valutare il rischio e sua decomposizione in sotto-scenari;

2. stima dei fattori FAIR per ogni sotto-scenario attraverso la tecnica PERT;

3. generazione degli scenari attraverso la simulazione Monte Carlo;

4. interpretazione dei risultati.

Valutazione quantitativa: FAIR

1. Definizione dello scenario di cui si vuole valutare il rischio e sua decomposizione in sotto-scenari.

Il punto di partenza di un'analisi FAIR è l'individuazione di una situazione che espone l'organizzazione al rischio cyber; a questa situazione ci si riferisce con il termine "*scenario*". Lo scopo di ogni analisi FAIR è quindi quello di valutare il livello di rischio associato al determinato scenario.

Valutazione quantitativa: FAIR

1. Definizione dello scenario di cui si vuole valutare il rischio e sua decomposizione in sotto-scenari.

Il punto di partenza di un'analisi FAIR è l'individuazione di una situazione che espone l'organizzazione al rischio cyber; a questa situazione ci si riferisce con il termine "*scenario*". Lo scopo di ogni analisi FAIR è quindi quello di valutare il livello di rischio associato al determinato scenario.

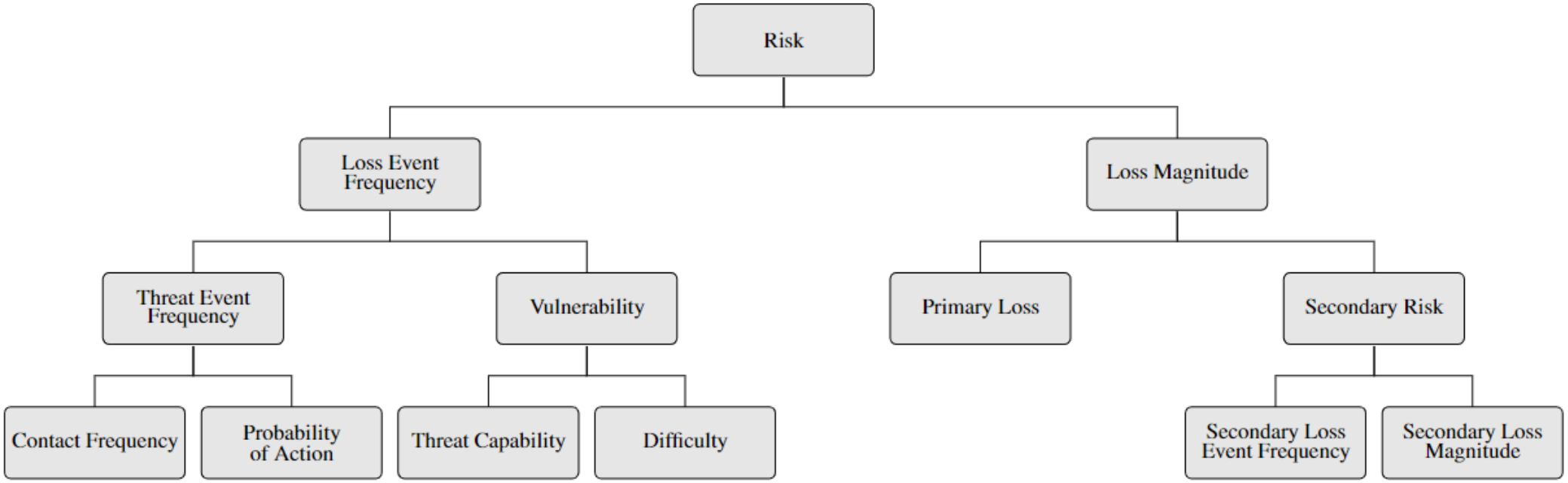
Una volta individuato lo scenario, questo viene raffinato e decomposto in sotto-scenari in base a quattro elementi:

- L'asset a rischio
- Gli agenti responsabili della minaccia
- La tipologia di minaccia
- L'effetto

Valutazione quantitativa: FAIR

2. Stima dei fattori FAIR per ogni sotto-scenario attraverso la tecnica PERT.

Il metodo FAIR definisce un'ontologia per il rischio in cui ogni elemento dell'ontologia rappresenta un fattore e i livelli dell'ontologia rappresentano delle successive decomposizioni in fattori, di livello tanto più basso quanto più si scende nella gerarchia a partire dall'alto.



Valutazione quantitativa: FAIR

2. Stima dei fattori FAIR per ogni sotto-scenario attraverso la tecnica PERT.

I fattori che rappresentano una perdita monetaria, ovvero Primary Loss e Secondary Loss Magnitude, sono inoltre ulteriormente decomposti in sei forme di perdita:

- Productivity - perdite dovute a una riduzione della capacità dell'organizzazione di perseguire i suoi obiettivi (produzione/erogazione di prodotti/servizi) e dal dover pagare i dipendenti nonostante non siano in grado di lavorare;

Valutazione quantitativa: FAIR

2. Stima dei fattori FAIR per ogni sotto-scenario attraverso la tecnica PERT.

I fattori che rappresentano una perdita monetaria, ovvero Primary Loss e Secondary Loss Magnitude, sono inoltre ulteriormente decomposti in sei forme di perdita:

- Productivity - perdite dovute a una riduzione della capacità dell'organizzazione di perseguire i suoi obiettivi (produzione/erogazione di prodotti/servizi) e dal dover pagare i dipendenti nonostante non siano in grado di lavorare;
- Response - perdite associate alla gestione dell'evento (meeting, investigazione, analisi forense, …);

Valutazione quantitativa: FAIR

2. Stima dei fattori FAIR per ogni sotto-scenario attraverso la tecnica PERT.

I fattori che rappresentano una perdita monetaria, ovvero Primary Loss e Secondary Loss Magnitude, sono inoltre ulteriormente decomposti in sei forme di perdita:

- Productivity - perdite dovute a una riduzione della capacità dell'organizzazione di perseguire i suoi obiettivi (produzione/erogazione di prodotti/servizi) e dal dover pagare i dipendenti nonostante non siano in grado di lavorare;
- Response - perdite associate alla gestione dell'evento (meeting, investigazione, analisi forense, …);
- Replacement - perdite legate al dover rimpiazzare risorse fisiche, dipendenti, …;

Valutazione quantitativa: FAIR

2. Stima dei fattori FAIR per ogni sotto-scenario attraverso la tecnica PERT.

I fattori che rappresentano una perdita monetaria, ovvero Primary Loss e Secondary Loss Magnitude, sono inoltre ulteriormente decomposti in sei forme di perdita:

- Productivity - perdite dovute a una riduzione della capacità dell'organizzazione di perseguire i suoi obiettivi (produzione/erogazione di prodotti/servizi) e dal dover pagare i dipendenti nonostante non siano in grado di lavorare;
- Response - perdite associate alla gestione dell'evento (meeting, investigazione, analisi forense, …);
- Replacement - perdite legate al dover rimpiazzare risorse fisiche, dipendenti, …;
- Competitive Advantage - perdite legate a proprietà intellettuale, brevetti, informazioni di mercato, …;

Valutazione quantitativa: FAIR

2. Stima dei fattori FAIR per ogni sotto-scenario attraverso la tecnica PERT.

I fattori che rappresentano una perdita monetaria, ovvero Primary Loss e Secondary Loss Magnitude, sono inoltre ulteriormente decomposti in sei forme di perdita:

- Productivity - perdite dovute a una riduzione della capacità dell'organizzazione di perseguire i suoi obiettivi (produzione/erogazione di prodotti/servizi) e dal dover pagare i dipendenti nonostante non siano in grado di lavorare;
- Response - perdite associate alla gestione dell'evento (meeting, investigazione, analisi forense, …);
- Replacement - perdite legate al dover rimpiazzare risorse fisiche, dipendenti, …;
- Competitive Advantage - perdite legate a proprietà intellettuale, brevetti, informazioni di mercato, …;
- Fines & Judgements - perdite legate a multe o cause legali;

Valutazione quantitativa: FAIR

2. Stima dei fattori FAIR per ogni sotto-scenario attraverso la tecnica PERT.

I fattori che rappresentano una perdita monetaria, ovvero Primary Loss e Secondary Loss Magnitude, sono inoltre ulteriormente decomposti in sei forme di perdita:

- Productivity - perdite dovute a una riduzione della capacità dell'organizzazione di perseguire i suoi obiettivi (produzione/erogazione di prodotti/servizi) e dal dover pagare i dipendenti nonostante non siano in grado di lavorare;
- Response - perdite associate alla gestione dell'evento (meeting, investigazione, analisi forense, …);
- Replacement - perdite legate al dover rimpiazzare risorse fisiche, dipendenti, …;
- Competitive Advantage - perdite legate a proprietà intellettuale, brevetti, informazioni di mercato, …;
- Fines & Judgements - perdite legate a multe o cause legali;
- Reputation - perdite dovute alla riduzione della quota di mercato, all'abbassamento del valore delle azioni, all'aumento del costo del capitale, alla perdita di clienti o ad una maggiore difficoltà nel trattenere o assumere dipendenti.

Valutazione quantitativa: FAIR

2. Stima dei fattori FAIR per ogni sotto-scenario attraverso la tecnica PERT.

Distribuzione per la generazione dei campioni

Alla base dell'analisi si ha la cosiddetta distribuzione PERT ("Program Evaluation and Review Technique"). La distribuzione PERT è definita da quattro parametri: il minimo a, il massimo b, il valore più probabile m e la confidenza λ. Il valore atteso della distribuzione è:

$$\mu = \frac{a + \lambda m + b}{\lambda + 2}$$

mentre la deviazione standard è:

$$\sigma = \frac{b - a}{\lambda + 2}$$

Valutazione quantitativa: FAIR

2. Stima dei fattori FAIR per ogni sotto-scenario attraverso la tecnica PERT.

La distribuzione PERT, che è una distribuzione discreta, può essere descritta tramite una distribuzione continua: la distribuzione beta a quattro parametri B(a,b,α,β), dove a e b assumono gli stessi valori di quelli specificati per la distribuzione PERT e α,β sono parametri di forma. La densità di probabilità (Probability Density Function, PDF) di B(a,b,α,β), è la seguente:

$$f(x) = \frac{(x-a)^{\alpha-1}(b-x)^{\beta-1}}{\mathrm{B}(\alpha,\beta)(b-a)^{\alpha+\beta-1}}$$

dove:

$$\mathrm{B}(\alpha,\beta) = \int_0^1 x^{\alpha-1}(1-x)^{\beta-1}\,dx$$

È possibile ottenere i parametri di forma dalla media e dalla varianza di una distribuzione PERT come segue:

$$\alpha = \frac{\mu-a}{b-a}\left[\frac{(\mu-a)(b-\mu)}{\sigma^2} - 1\right]$$

$$\beta = \alpha\frac{b-\mu}{\mu-a}$$

Valutazione quantitativa: FAIR

3. Generazione degli scenari attraverso la simulazione Monte Carlo.

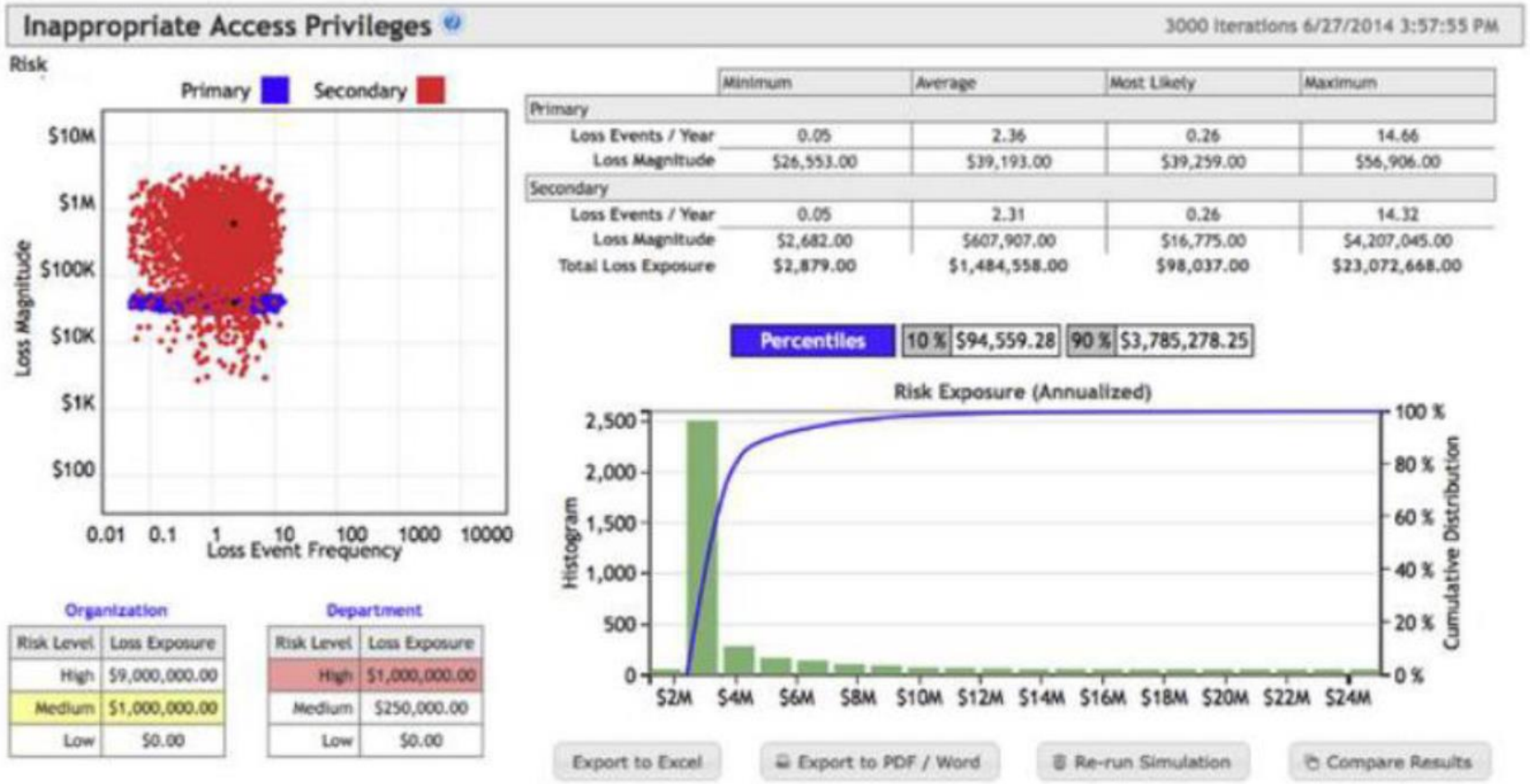
Le stime dei fattori vengono usate come input per la simulazione Monte Carlo. In questo caso di variabili aleatorie di interesse ve ne sono cinque per ogni scenario:

- La frequenza con cui si ha una perdita primaria (n_{pp});
- L'entità della perdita primaria associata ad un singolo evento (PP_1);

Valutazione quantitativa: FAIR

4. Interpretazione dei risultati.

I risultati della simulazione Monte Carlo vengono presentati attraverso diverse rappresentazioni in formato grafico o tabella.



Valutazione quantitativa: FAIR

4. Interpretazione dei risultati.

Legenda:

- Grafico a dispersione o scatterplot: riporta i punti (npp, PP1) e (nps, PS1) per ciascuno scenario generato con la simulazione Monte Carlo, in modo tale da rendere più immediato il confronto tra la perdita primaria e la perdita secondaria;

Valutazione quantitativa: FAIR

4. Interpretazione dei risultati.

Legenda:

- Grafico a dispersione o scatterplot: riporta i punti (npp, PP1) e (nps, PS1) per ciascuno scenario generato con la simulazione Monte Carlo, in modo tale da rendere più immediato il confronto tra la perdita primaria e la perdita secondaria;
- Tabella riassuntiva: riporta i valori minimo, medio, più verosimile e massimo ottenuti con la simulazione Monte Carlo per ciascuna delle variabili di interesse. Si noti che i valori minimo, medio, più verosimile e massimo della Total Loss Exposure devono essere calcolati secondo tutti i risultati della simulazione Monte Carlo e non possono essere calcolati solo a partire dai valori minimo, medio, più verosimile e massimo di Primary loss events, Primary loss magnitude, Secondary loss events, Secondary loss magnitude;

Valutazione quantitativa: FAIR

4. Interpretazione dei risultati.

Legenda:

- Grafico a dispersione o scatterplot: riporta i punti (npp, PP1) e (nps, PS1) per ciascuno scenario generato con la simulazione Monte Carlo, in modo tale da rendere più immediato il confronto tra la perdita primaria e la perdita secondaria;
- Tabella riassuntiva: riporta i valori minimo, medio, più verosimile e massimo ottenuti con la simulazione Monte Carlo per ciascuna delle variabili di interesse. Si noti che i valori minimo, medio, più verosimile e massimo della Total Loss Exposure devono essere calcolati secondo tutti i risultati della simulazione Monte Carlo e non possono essere calcolati solo a partire dai valori minimo, medio, più verosimile e massimo di Primary loss events, Primary loss magnitude, Secondary loss events, Secondary loss magnitude;
- Percentili: rappresentano il 10° e il 90° percentile della perdita totale (P). Il 10° percentile della perdita totale è il valore sotto il quale si trova il 10% dei valori di perdita totale ottenuti con la simulazione Monte Carlo. Definizione analoga vale per il 90° percentile.

MAGIC

MAGIC: a **M**ethod for **A**ssessin**G** cyber **I**ncidents o**C**currence

Lavoro svolto nell'ambito del progetto "Cyber Risk Assessment Models and Algorithms (CybeRAMA)" finanziato dalla Fondazione Cassa di Risparmio di Verona Vicenza Belluno e Ancona

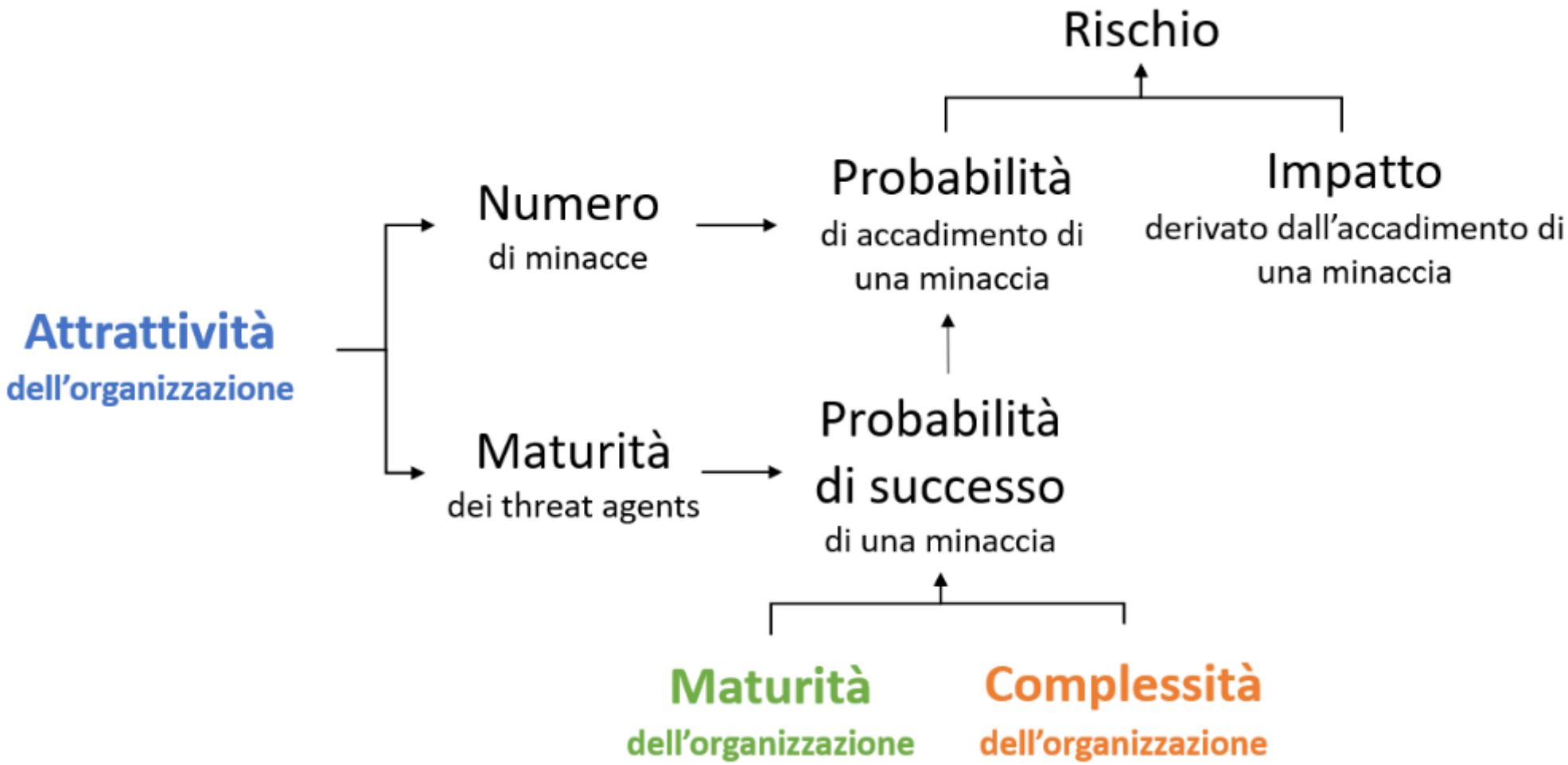
- M. Battaglioni, G. Rafaiani, F. Chiaraluce and M. Baldi, "MAGIC: A Method for Assessing Cyber Incidents Occurrence," in IEEE Access, vol. 10, pp. 73458-73473, 2022, doi: 10.1109/ACCESS.2022.3189777.
- G. Rafaiani, M. Battaglioni, M. Baldi, F. Chiaraluce, G. Libertini, L. Spalazzi, and G. Cancellieri, "A functional approach to cyber risk assessment," in Proceedings AEIT 2021 International Annual conference, 2021
- G. Rafaiani, M. Battaglioni, M. Baldi, and F. Chiaraluce, "Cyber risk assessment: a pragmatic approach," in Proceedings ICITEE 21, 2021

MAGIC

- **MAGIC** è un metodo *quantitativo* semplice ed efficiente per valutare il rischio cyber
- Mira a risolvere uno dei principali inconvenienti della maggior parte dei metodi di valutazione esistenti (incluso HTMA):

come stimare, nel modo più oggettivo possible, la probabilità di accadimento degli eventi?

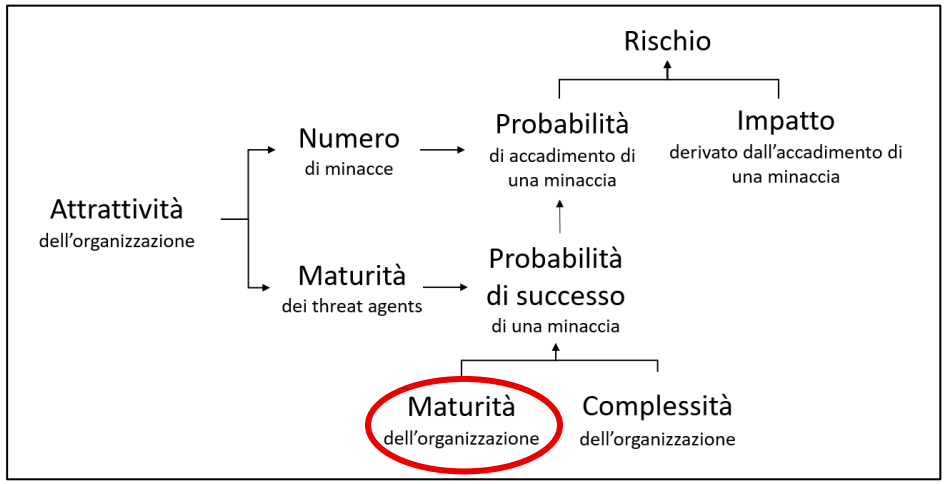
MAGIC


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

- **Maturità dell'organizzazione**

Valutazione della postura di un'organizzazione riguardo il rischio cyber



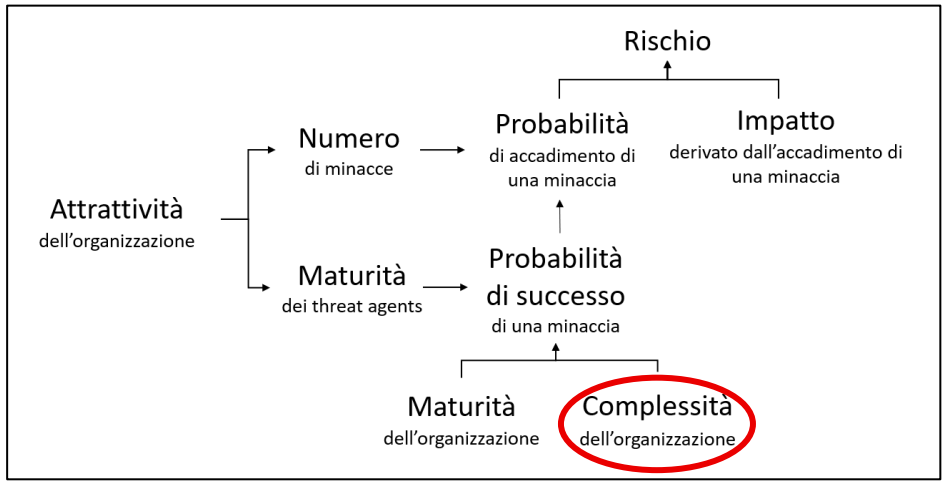
- *COME?* Valutiamo il livello di compliance dell'organizzazione ai controlli di uno o più cybersecurity frameworks. Otteniamo un indice tra 0 e 10

- A seconda dei framework di riferimento considerati si possono stimare diversi tipi di rischio (data protection, attacchi cyber…)

MAGIC

- **Complessità dell'organizzazione**

Valutazione della complessità dell'infrastruttura tecnologica dell'organizzazione, in termini di livello di «intricatezza»



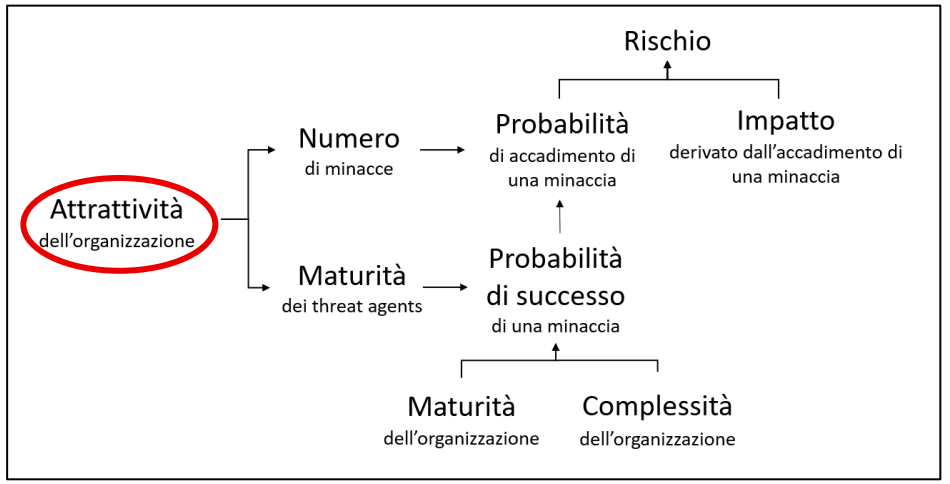
- Il rischio a cui è soggetta un'organizzazione non è dovuto solamente alle misure che mette in atto per proteggersi, ma anche dal suo livello di complessità

- *COME?* Valutiamo il livello di compliance dell'organizzazione a un set di controlli selezionati tramite esperti e letteratura. Otteniamo un indice tra 0 e 10

MAGIC

- **Attrattività dell'organizzazione**

Valutazione dell'interesse
che l'organizzazione causa
sui threat agents



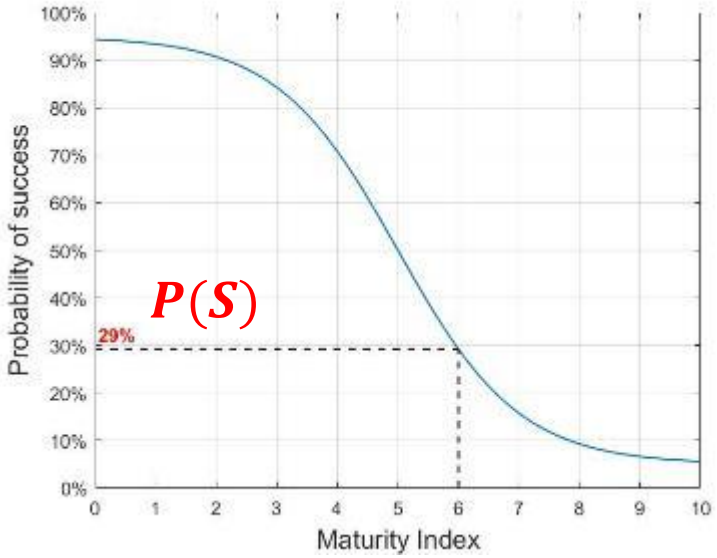
- Dipende dal *tipo* dell'organizzazione, dal tipo e dalla quantità di *dati* che processa. Influenza il numero di attacchi ricevuti, ma anche il tipo di attaccante

- *COME?* Classifichiamo i diversi tipi di organizzazioni in 5 categorie, a seconda di quanti attacchi hanno subito nell'ultimo anno rispetto al numero totale di attacchi

MAGIC

- **Probabilità di successo di una minaccia**

Valutazione della probabilità di successo di una minaccia attraverso una funzione logistica generalizzata



$$P(S) = A + \frac{K - A}{1 + e^{-B(x - x_0)}} \quad with\ 0 \le x \le 10, B < 0$$

Probabilità di successo $\boldsymbol{P(S)}$ ➡ $\boldsymbol{p} = P(S) \times a$

MAGIC

- **Probabilità di accadimento di *minacce multiple***

Valutazione della probabilità di accadimento di minacce multiple (non rilevate) attraverso la combinazione di alcune distribuzioni di probabilità

$$\Pr(S = s \mid N = n) = \int_{p_m}^{p_M} \mathrm{BINOM}(n, s, p)\, \mathrm{PERT}(p)\mathrm{d}p \qquad \Pr(N = n) = \mathrm{BINOM}\left(t, n, \frac{n_{\mathrm{avg}}}{t}\right)$$

$$\Pr(S = s) = \sum_{n=1}^{t} \Pr(S = s \mid N = n) \Pr(N = n)$$

MAGIC

- **Probabilità di accadimento di una *minaccia singola***

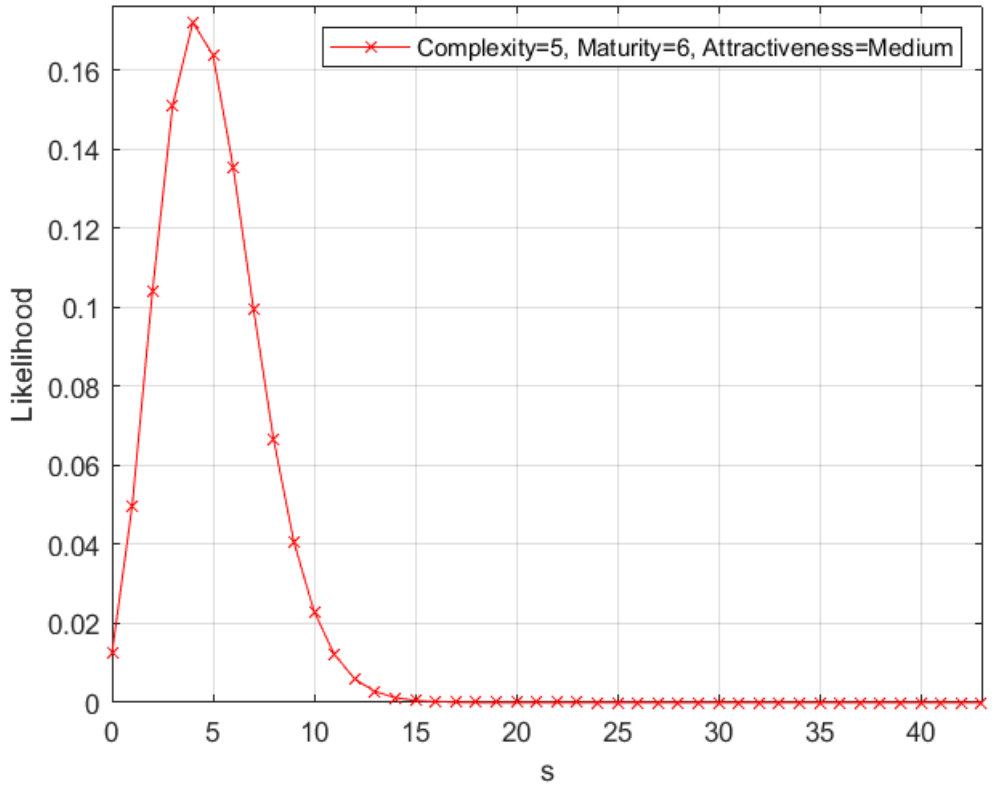
Valutazione della probabilità di accadimento di una minaccia singola (rilevata) attraverso la combinazione di alcune distribuzioni di probabilità

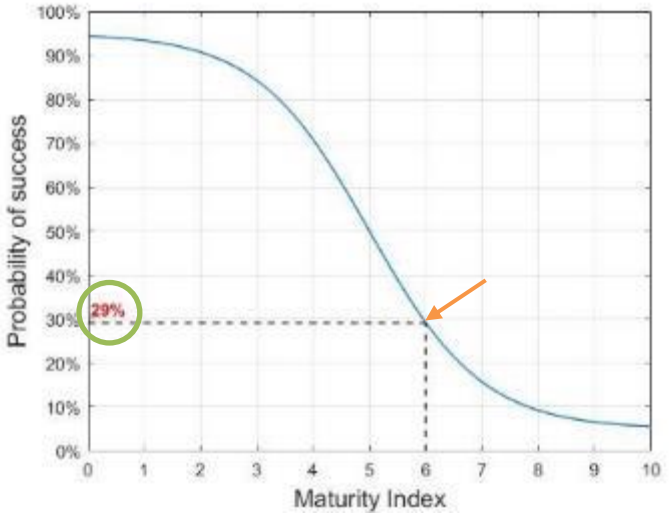
$$\Pr(S = s \mid N = n) = \int_{p_m}^{p_M} \mathrm{GEOM}(n, s, p)\,\mathrm{PERT}(p)\,\mathrm{d}p \qquad \Pr(N = n) = \mathrm{BINOM}\left(t, n, \frac{n_{\mathrm{avg}}}{t}\right)$$

$$\Pr(S = 1) = \sum_{n=1}^{t} \Pr(S = 1 \mid N = n)\,\Pr(N = n)$$

MAGIC - Esempio

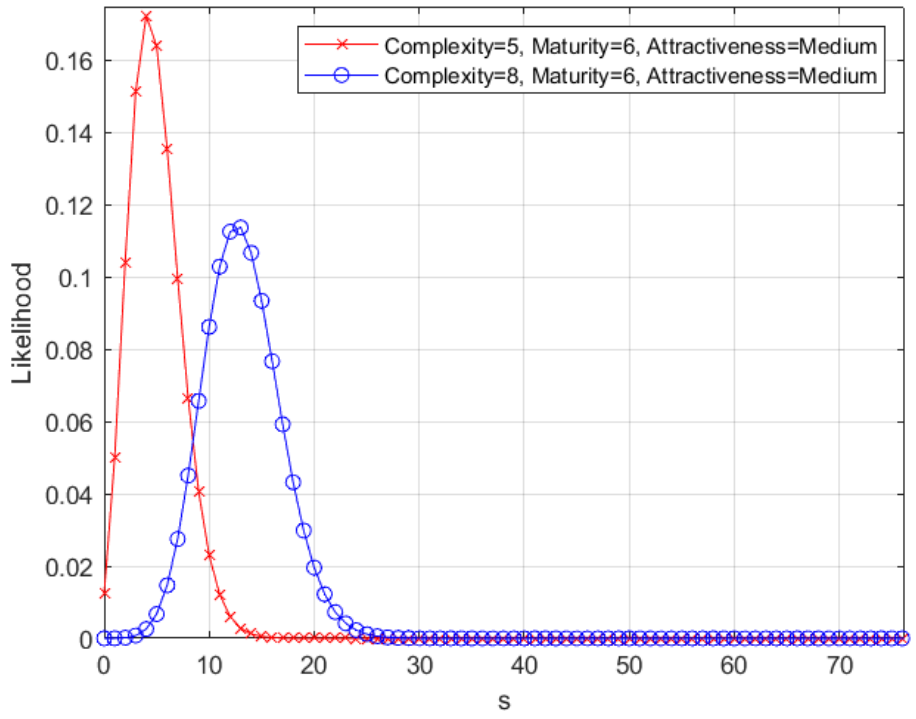
- **Complessità:** 5
- **Maturità:** 6
- **Attrattività:** Media

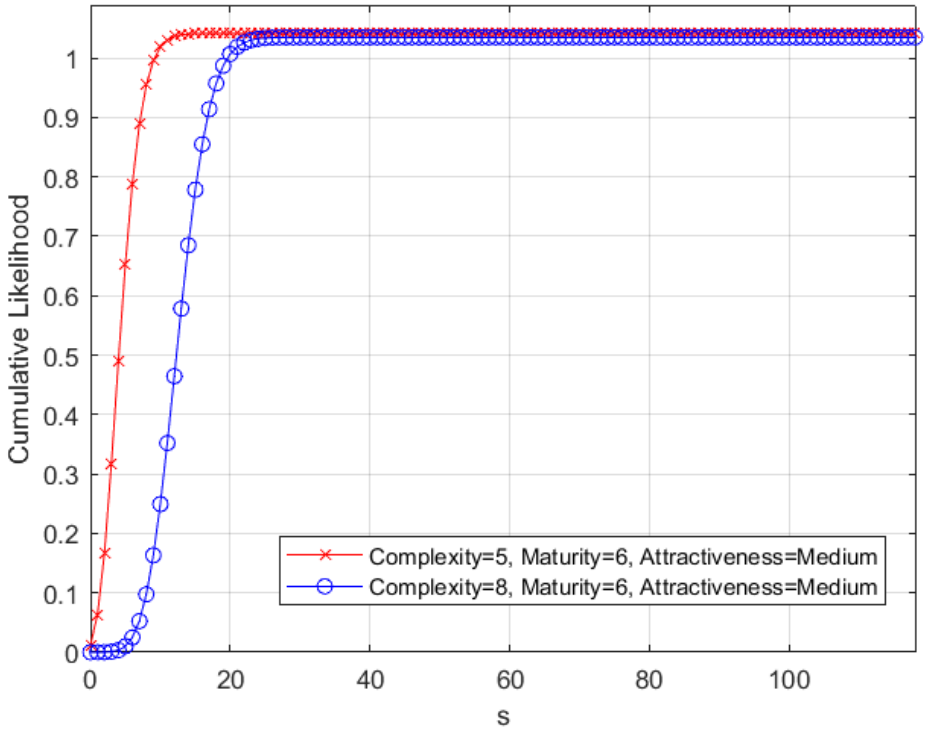




MAGIC - Esempio

- **Complessità:** 5 -8
- **Maturità:** 6
- **Attrattività:** Media





MAGIC - HTMA

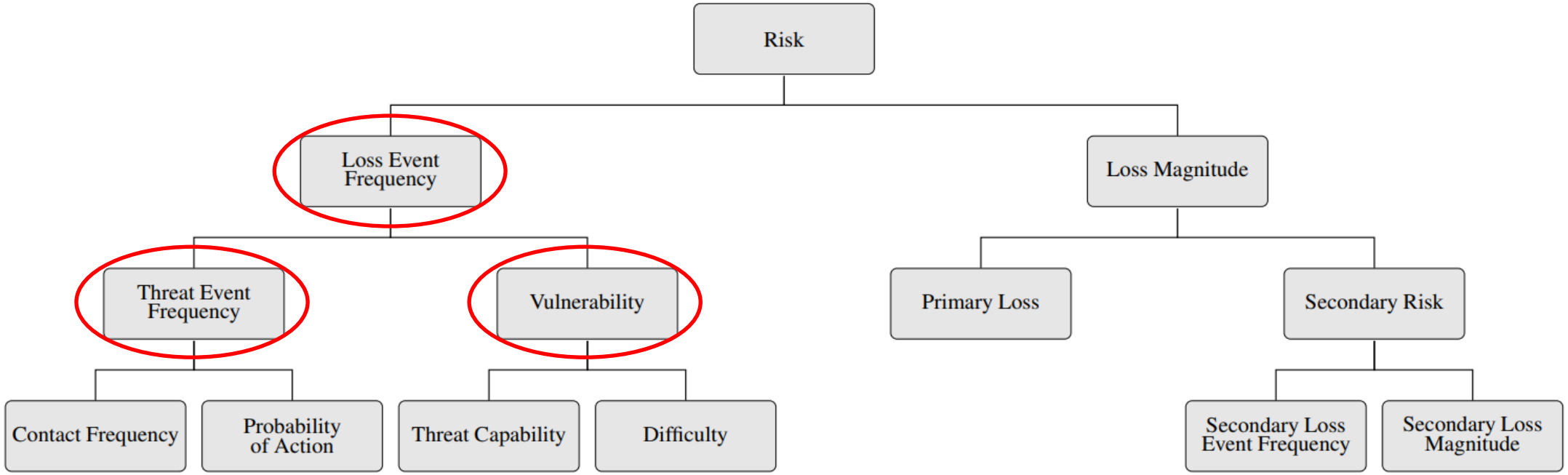
- Con il metodo della curva logistica, abbiamo ottenuto la probabilità di accadimento di una qualsiasi minaccia in un determinato periodo di tempo

Cosa possiamo fare per ottenere una LEC?
Simulazione Monte Carlo!

- Per applicare la simulazione Monte Carlo (come per il metodo HTMA), abbiamo bisogno di una lista di eventi, con probabilità di accadimento e impatti

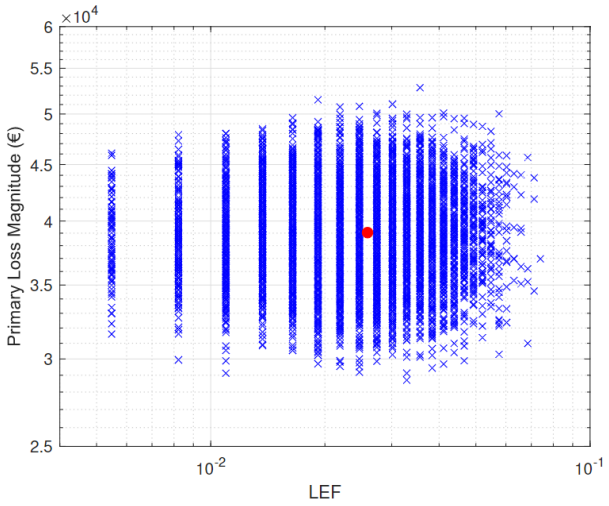
- Ma, ora, le probabilità di accadimento non sono più correlate al parere di esperti e/o a dati storici, ma sono relative all'attuale postura cyber dell'organizzazione

MAGIC - FAIR


Risk
Loss Event Frequency
Loss Magnitude
Threat Event Frequency
Vulnerability
Primary Loss
Secondary Risk
Contact Frequency
Probability of Action
Threat Capability
Difficulty
Secondary Loss Event Frequency
Secondary Loss Magnitude

MAGIC - FAIR

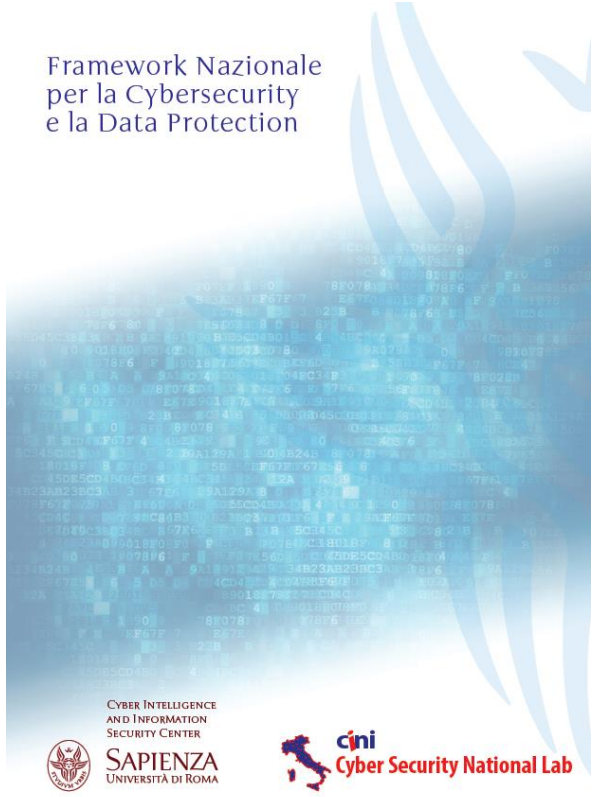
- Si stima la probabilità di accadimento di *s* eventi sfavorevoli
- Tramite una procedura di campionamento, si ricava la relativa frequenza (LEF)
- La simulazione Monte Carlo può restituire risultati in forma diversa



	Minimum	Mean	Mode	Maximum
Primary Loss Events per year	1	9.5	8	27
Primary Loss Magnitude (€)	28, 709	39, 045	32, 948	52, 822
Total Loss Exposure (€)	35, 369	369, 260	295, 520	1, 141, 600

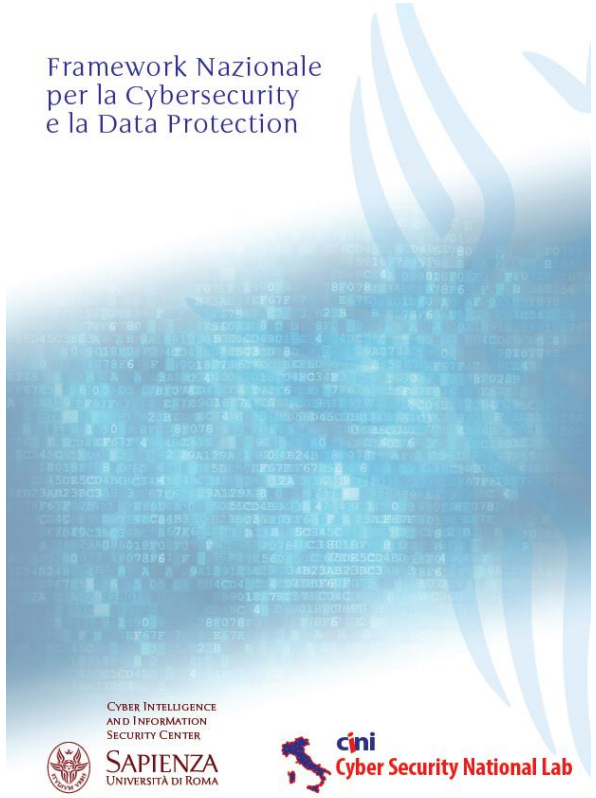
Strategia nazionale per la cyber security

Framework nazionale per la cyber security e la data protection

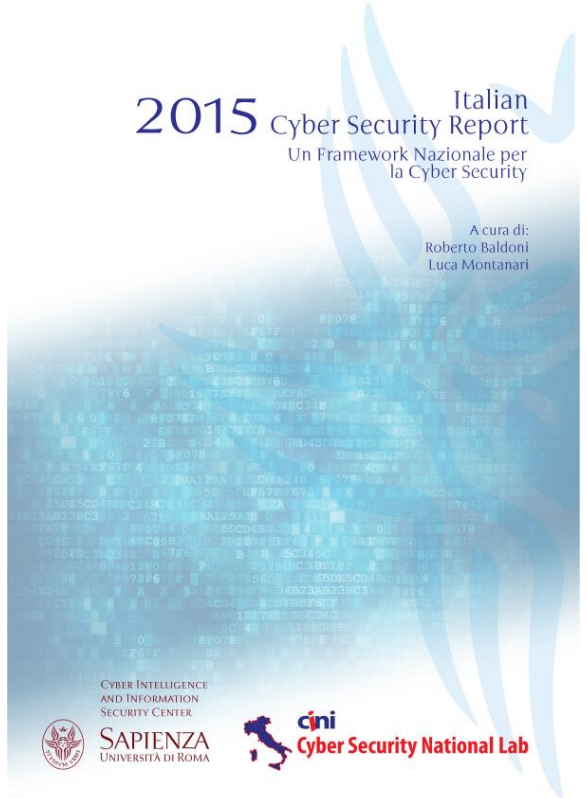


Strumento di autovalutazione del rischio cyber

Framework nazionale per la cyber security e la data protection



vs.



- Rispetto alla versione precedente, la versione 2.0 introduce contributi volti a cogliere gli aspetti fondamentali legati alla protezione dei dati secondo quanto previsto nel Regolamento Generale sulla Protezione dei Dati (GDPR – d'ora in avanti: *Regolamento*).