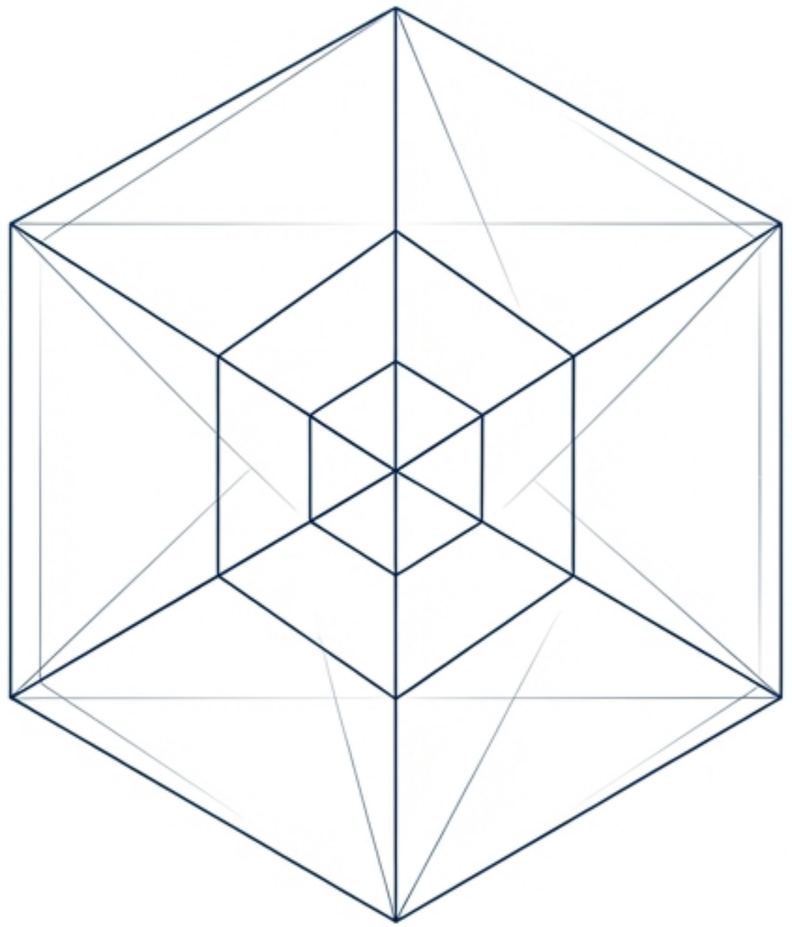
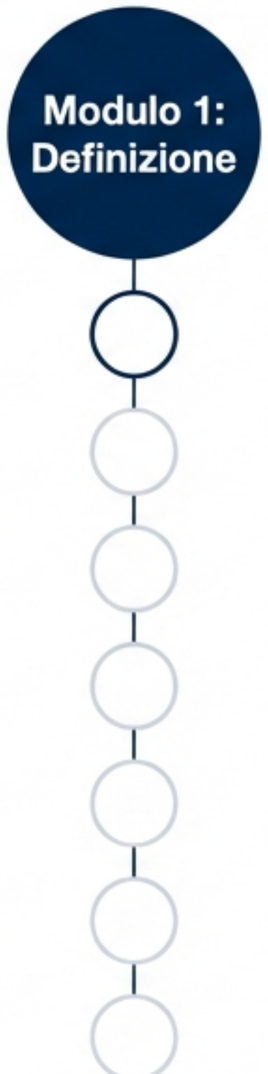
Definizione e Gestione del Rischio Cyber

MODULO 1: CONCETTI FONDAMENTALI E TASSONOMIA



Obiettivi del Modulo e **Contesto del Corso**

Questa presentazione costituisce il primo di otto moduli dedicati alla gestione del rischio cyber. L’obiettivo primario è stabilire una definizione rigorosa di ‘rischio’ e identificare le grandezze fondamentali necessarie per la sua gestione.



Il rischio è un concetto quotidiano, ma in ambito accademico e ingegneristico richiede una formalizzazione precisa per passare dalla percezione soggettiva alla valutazione oggettiva.

La Definizione Formale: Norma UNI 11230

Secondo l'Ente Nazionale Italiano di Normazione (UNI 11230), il rischio è definito come:

L'insieme delle possibilità di un evento e delle sue conseguenze sugli obiettivi.

Rischio = Possibilità (Probabilità) × Conseguenze (Impatto)

La frequenza o verosimiglianza dell'accadimento.

L'effetto dell'evento sugli obiettivi preposti.

Questa definizione funge da vocabolario standard per l'intera trattazione.

Accezione Negativa vs. Accezione Neutra

Percezione Comune

Fonti generaliste (Wikipedia, ChatGPT) definiscono il rischio come la potenzialità di un evento indesiderabile, associato esclusivamente a perdite o danni.

Equazione:
Rischio = Evento Negativo

Visione Tecnica/Finanziaria

La norma UNI 11230 offre una definizione generica e neutra. In ambiti come la Finanza o la Teoria dei Giochi, il rischio è legato alle conseguenze, che possono essere positive (Opportunità).

Binomio Rischio-Rendimento: Gli investimenti con il maggior ritorno potenziale sono teoricamente associati a un rischio maggiore.

Sebbene nel Cyber Risk le conseguenze siano quasi sempre negative (attacchi), è fondamentale comprendere la neutralità teorica del concetto.

Tassonomia dei Rischi

Rischi Naturali

Catastrofi, alluvioni, terremoti

Rischi Sociali

Criminalità, terrorismo

Rischi Finanziari

Investimenti, mercati

Rischi Competitivi

Dinamiche di mercato

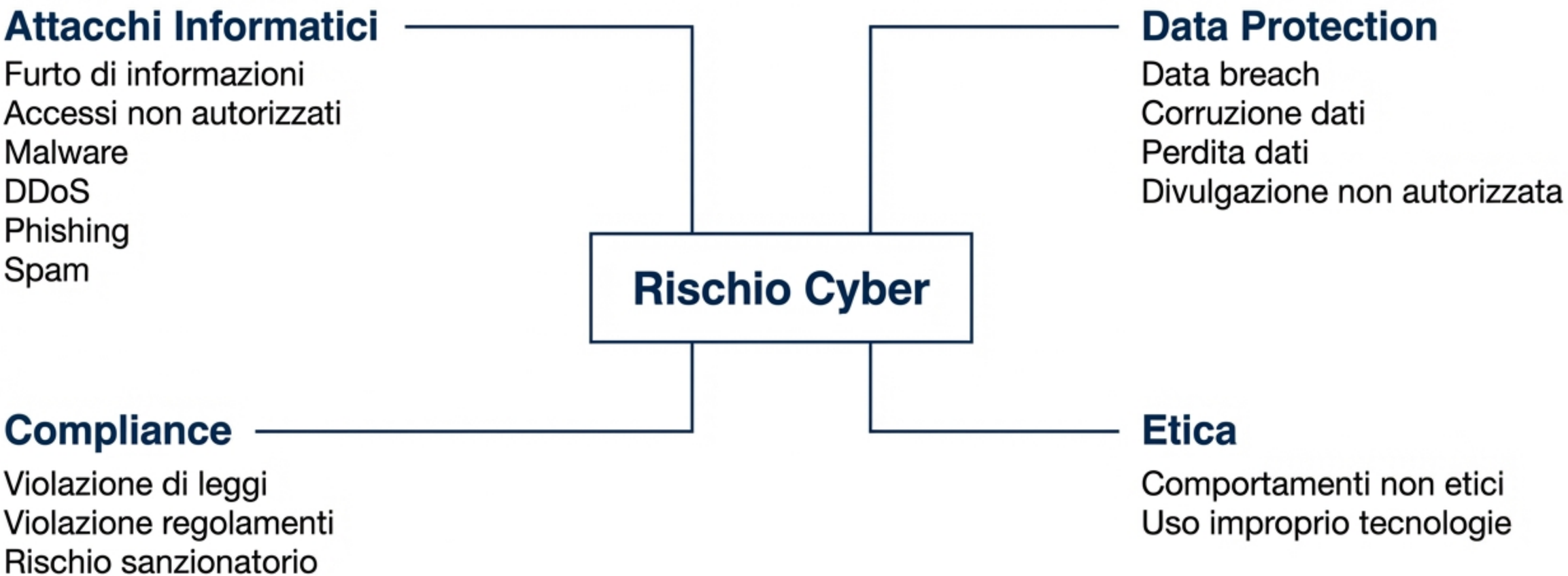
Rischi Fisici

Incidenti sul lavoro, accessi non autorizzati

Rischi Cyber

Focus del Corso. Legati al dominio cibernetico e alla sicurezza delle informazioni.

Il Dominio del Rischio Cyber



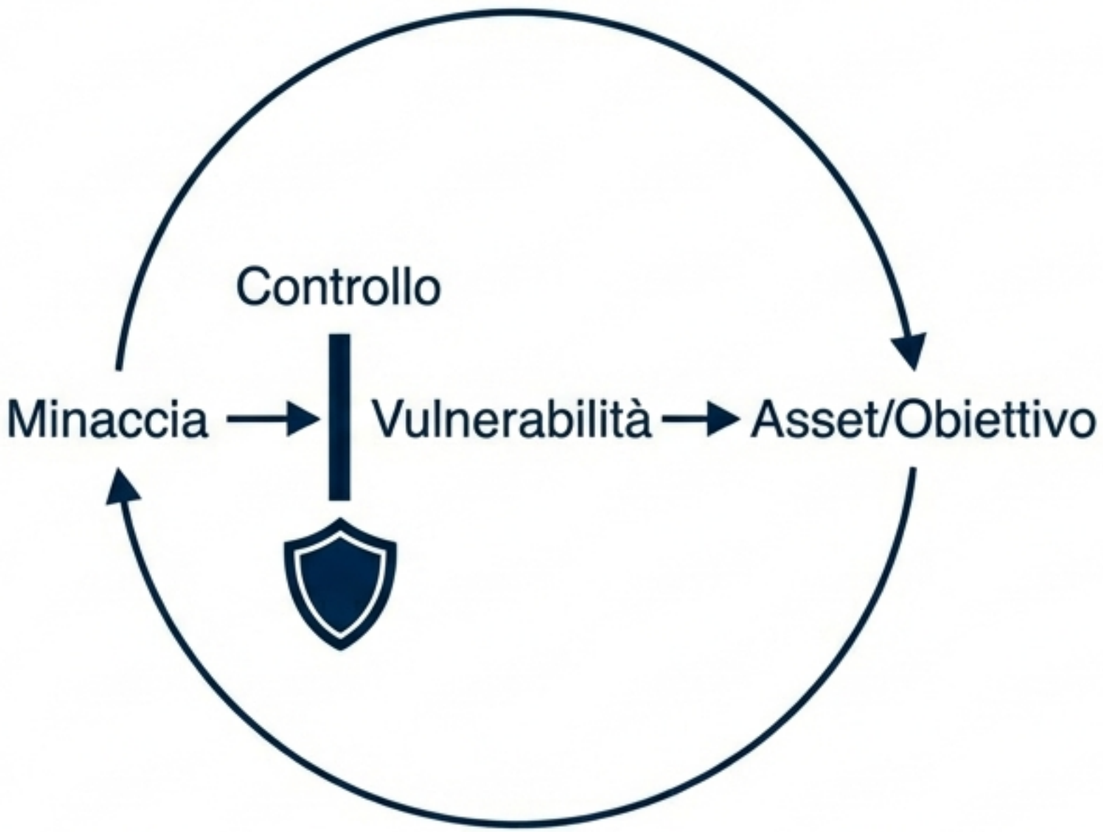
Terminologia Essenziale (UNI 11230)

Probabilità: Misura o stima della possibilità che un evento ha di verificarsi.

Controllo: Una misura che mantiene (se il livello è adeguato) o modifica il rischio.

Minaccia: Causa o origine di un danno potenziale (es. un attaccante esterno, un virus).

Vulnerabilità: Debolezza di un asset o di un controllo che può essere sfruttata da una minaccia (es. mancanza di antivirus).



La Sfida della Stima Probabilistica

Approccio Classico

Probabilità nota e calcolabile (es. 1/6).
Dati perfetti.

Approccio Cyber

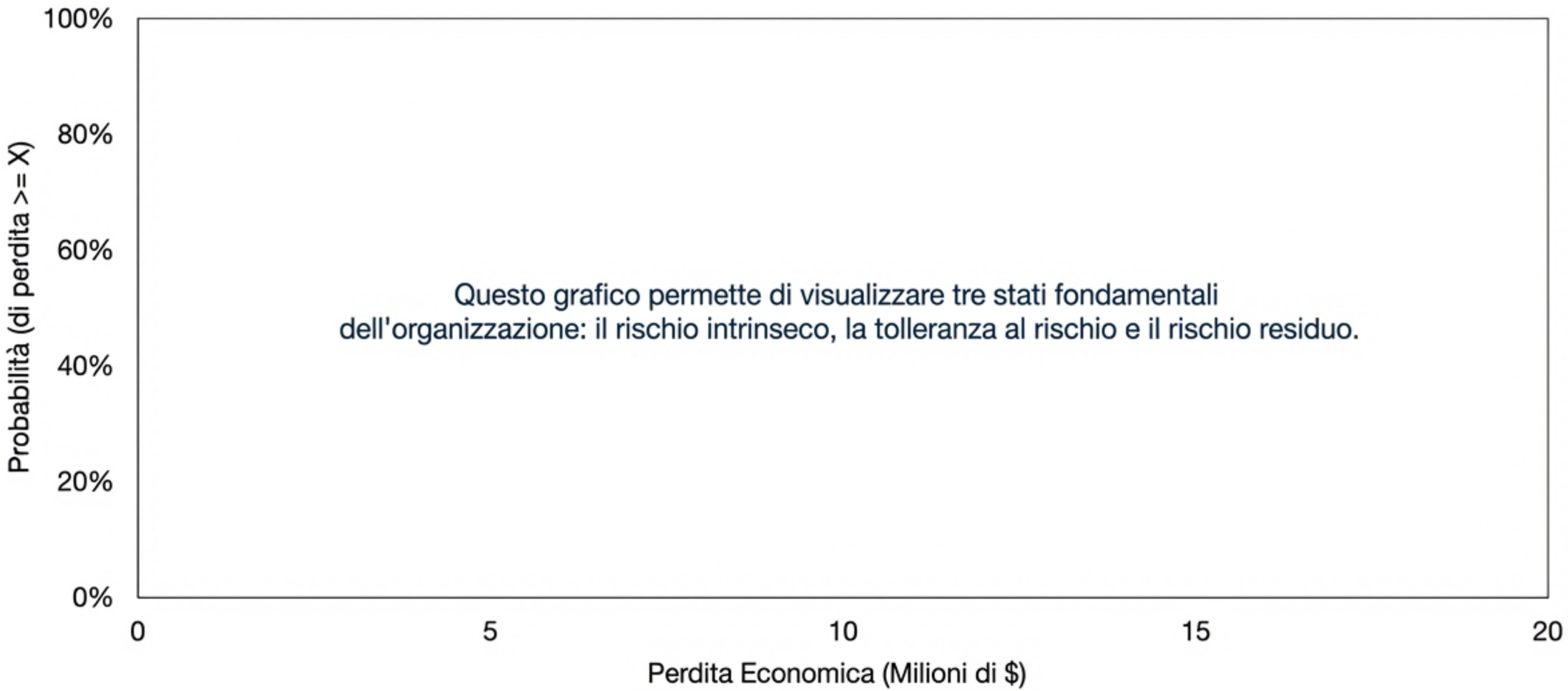
Probabilità epistemica (es. Meteo/Attacchi).
Non possiamo calcolare con precisione l'evento futuro.

Key Challenges nel Cyber Risk:

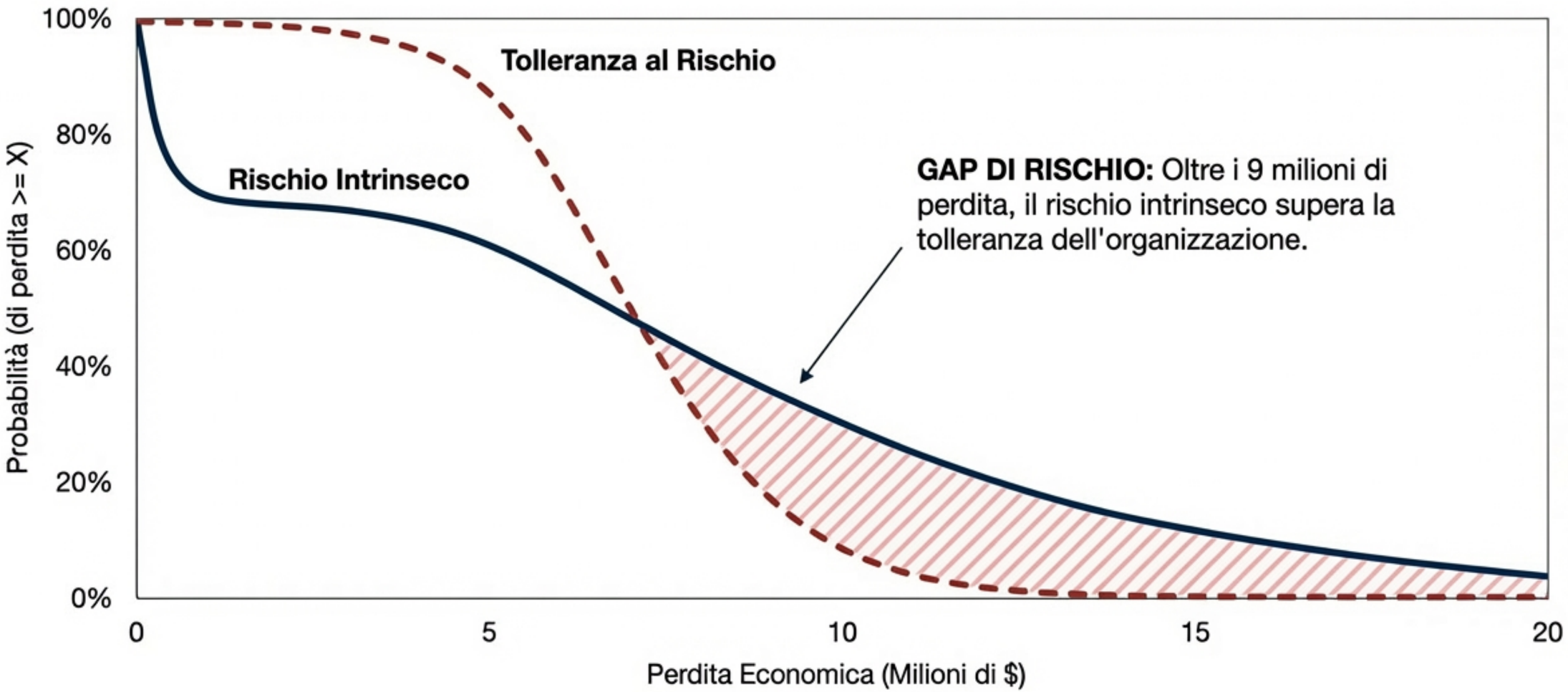
- Mancanza di Storico: Dati interni spesso assenti o non rilevati.
- Dati Non Strutturati: Eccesso di dati esterni (threat intelligence) difficili da correlare alla specifica organizzazione.
- Conclusione: Stimare la probabilità richiede tempo ed è spesso affetto da incertezza.

Valutazione Quantitativa: La Curva di Rischio

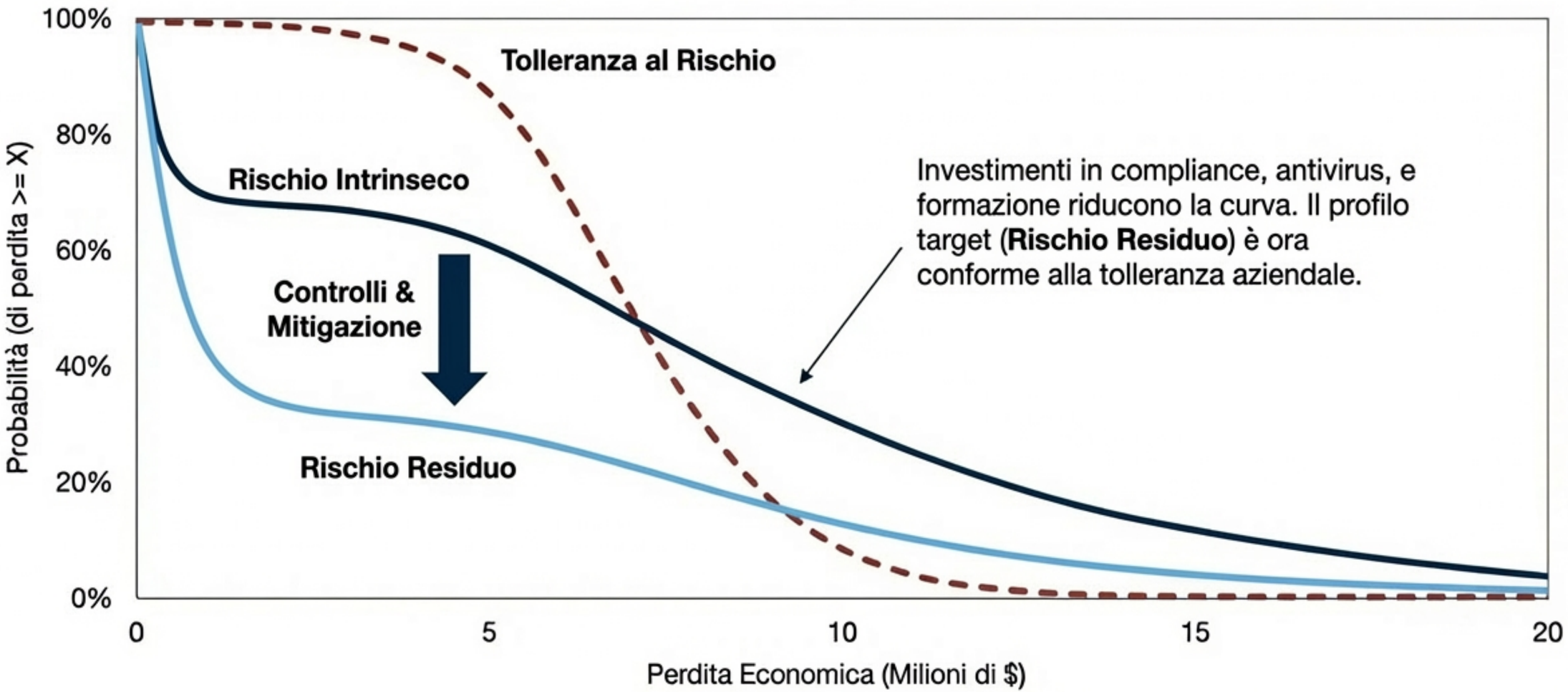
Setup del Modello Loss Exceedance



Analisi del Gap: Rischio Intrinseco vs. Tollerabile



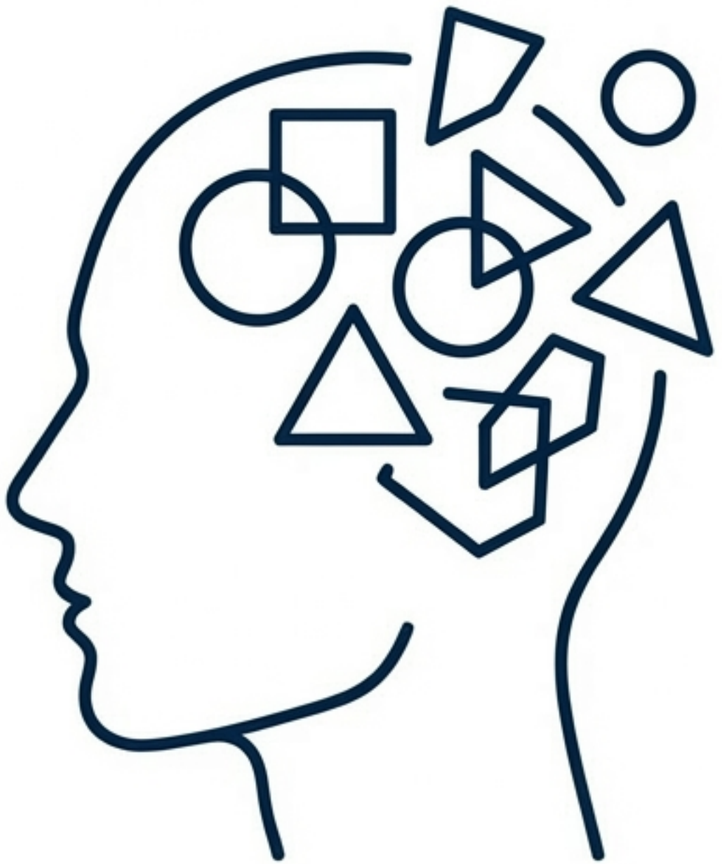
Il Rischio Residuo e l'Effetto dei Controlli



Il Fattore Umano: Introduzione alla Chindinica

Definizione:
La Chindinica (o scienza del pericolo) studia i meccanismi che si instaurano in ambienti complessi, come le organizzazioni.

Premessa Fondamentale:
- Ogni individuo ha una diversa propensione al rischio.
- La percezione del rischio è soggettiva.
- Questa soggettività influenza la valutazione al di là dei modelli matematici.



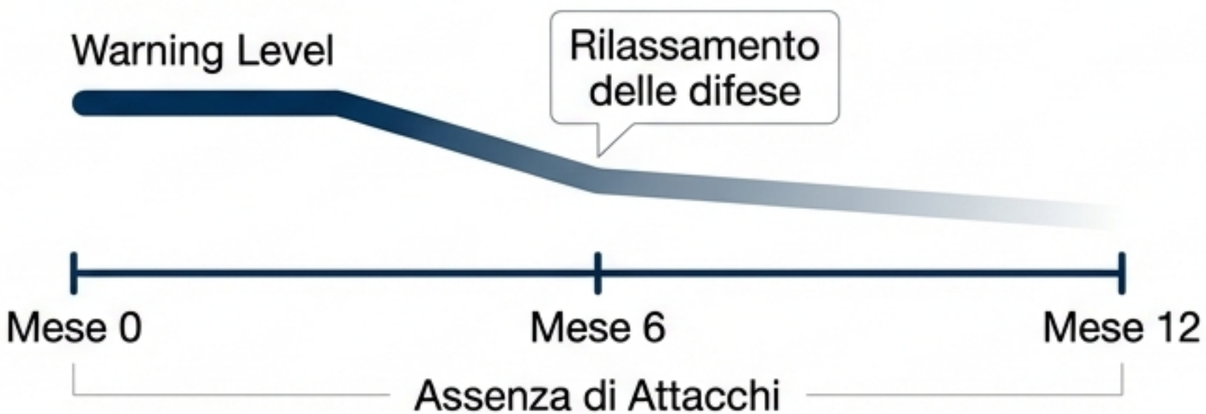
Le Leggi della Percezione del Rischio

Legge dell’Antipericolo

La gravità di un pericolo è accresciuta dalla sottostima della sua probabilità. Le organizzazioni tendono sistematicamente a sottostimare gli eventi avversi.

Legge dell’Assuefazione

Il costante confronto con rischi a bassa probabilità porta a una riduzione della percezione del rischio. L’assenza di attacchi per 6-12 mesi causa un “rilassamento” delle difese.



Assiomi della Chindinica

“Relatività della Misura”

Il rischio non può essere quantificato in modo assoluto. Le misurazioni dipendono strettamente dal contesto territoriale e temporale in cui l’individuo opera.

“Il Valore della Conoscenza”

La conoscenza riduce il rischio. La consapevolezza (*awareness*) diffusa a tutti i livelli dell’organizzazione è un fattore determinante per ridurre il potenziale impatto.

Sintesi del Modulo

R=PxI

Definizione

Il rischio è il prodotto di Probabilità x Impatto (UNI 11230). In teoria può essere neutro, ma nel Cyber è quasi sempre negativo.

Valutazione

La stima della probabilità cyber è complessa a causa della mancanza di dati strutturati e storici affidabili.

Analisi Quantitativa

Le curve di rischio (Intrinseco, Tollerabile, Residuo) permettono di visualizzare il 'Gap' e pianificare i controlli di mitigazione.

Soggettività

La Chindinica insegna che la percezione umana (assuefazione, sottostima) è una variabile critica da gestire insieme ai controlli tecnici.