Cyber-Resilienza per le PMI: il nuovo volto della sicurezza informatica alla luce della NIS2
20 Aprile 2026 · Verona

Cybersecurity: un cambio di prospettiva per proteggere il valore dell'impresa

Silvio Ranise
Università di Trento & Fondazione Bruno Kessler

FONDAZIONE BRUNO KESSLER

UNIVERSITÀ DI TRENTO

Oltre la “Conta dei Virus”

- Cambio di visione
  - Smettere di guardare ai “tentativi di attacco bloccati” (**metrica tecnica**) e iniziare a considerare l'impatto sul business (**metrica imprenditoriale**)
- Osservazione cruciale
  - In un'azienda digitalizzata, la **cybersecurity** non è un costo IT, ma una **componente della continuità operativa**

- **Obiettivo**
  - Imparare a decidere quanto investire basandosi su numeri, non sulla paura

Al Board **non** interessa **quanti attacchi** sono stati **bloccati**, ma **quanto tempo l'azienda rimarrà ferma** se uno solo di questi va a segno

https://www.briskinfosec.com/blogs/blogsdetail/Measuring-Cybersecurity-ROI-Through-Business-Resilience-Metrics

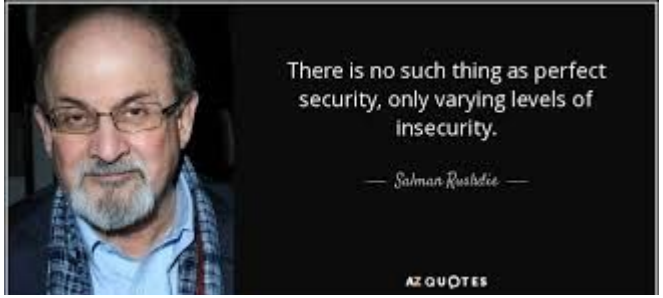
Quantificare la **perdita derivante da un mancato investimento** è complesso perché implica la **misurazione di un guadagno ipotetico** che non si è mai realizzato, **anziché una perdita reale** di capitale già posseduto

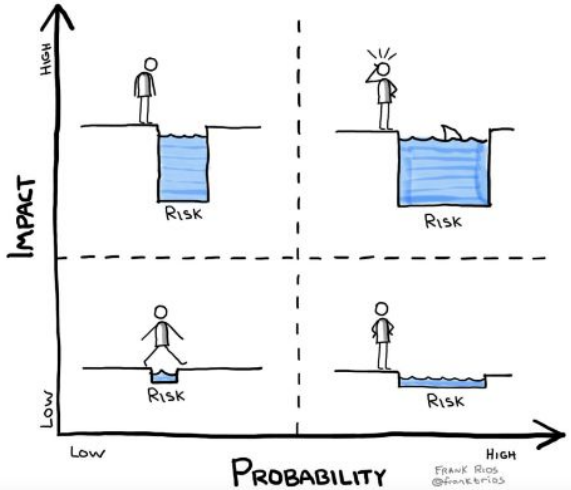
Sicurezza vs Rischio

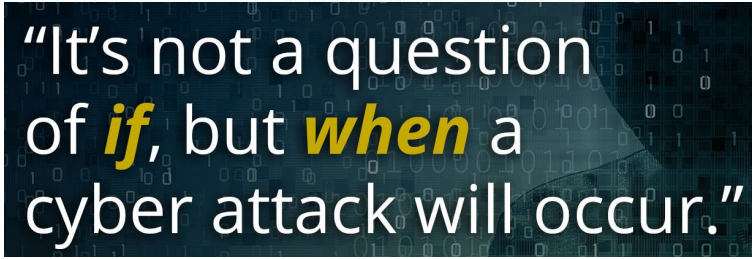
- In ambito digitale, il rischio zero non esiste
  - Nessun sistema, per quanto costoso, è inattaccabile al 100%
- Definizione di rischio
  - [**Probabilità evento dannoso accada**] x [**Impatto** (economico, operativo, legale)]
- Cambio di prospettiva:

difendere → gestire

  - Se accettiamo che la sicurezza perfetta è un'illusione, allora non cerchiamo più l'invulnerabilità, ma la **resilienza** (la **capacità di resistere e ripartire**)

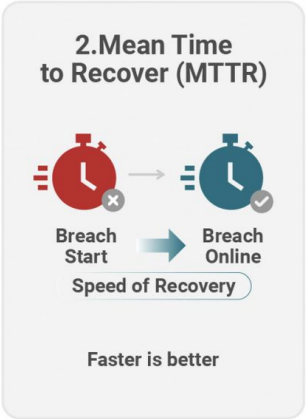


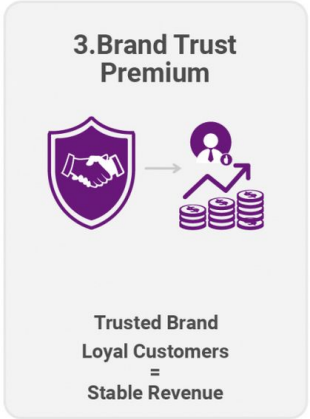




Cambio di prospettiva: tecnica → imprenditoriale

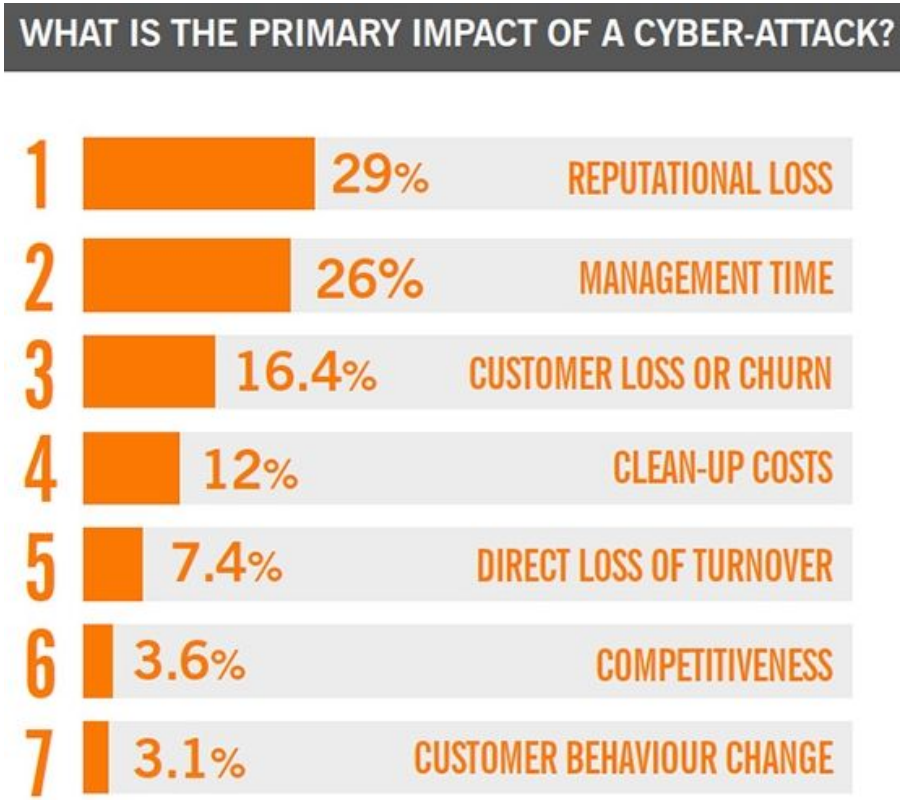
- Esposizione Finanziaria al Rischio (**Cyber Loss Expectancy**)
  - **Quanto denaro** potremmo perdere quest'anno a causa di un tipo di incidente?
    - Include anche il fatturato perso durante il tempo di recupero
  - Quanto può essere **frequente** quel tipo di incidente?
  - Quantificazione del rischio: [Frequenza] x [Quantità di denaro]
- Tempo di Recupero (**RTO - Recovery Time Objective**)
  - Se spegniamo tutto ora, **quanto tempo** serve per tornare a fatturare?
- Protezione **Asset e Business Process vitali**
  - Abbiamo protetto adeguatamente i dati e le attività produttive che generano profitto (clienti, segreti industriali, ordini) per mostrarci affidabili ai clienti?



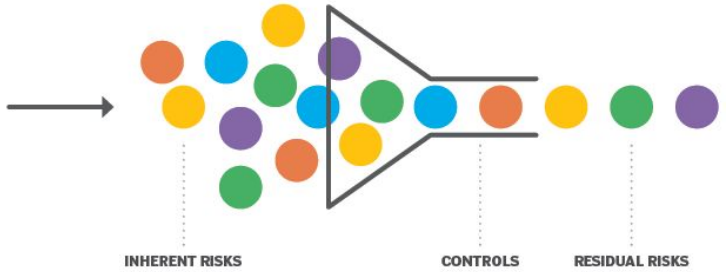


Quantificare il danno: costi

- **Immediati**: Incident response, ripristino sistemi, consulenze legali
- **Blocco**: Fermo produzione, penali contrattuali per ritardi nelle consegne
- **Silenziosi**: Danno d'immagine e perdita di quote di mercato a favore di competitor “più affidabili”
- **Derivanti da sanzioni**: Mancata conformità (GDPR, NIS2) aggiunge un peso economico diretto



Gestione del rischio



Possibili strategie di gestione

- **Avoid**: Eliminare l'attività rischiosa
  - Esempio: dismettere un server obsoleto che non può più essere aggiornato o rinunciare a un software gratuito ma non sicuro
- **Mitigate**: Abbassare probabilità e impatto adottando controlli di sicurezza
  - Tecnici: Implementare i controlli di sicurezza (MFA, backup, patch management)
  - Umani: formare i dipendenti (contro il phishing)
- **Accept**: Accettare il rischio coscientemente
  - Si applica quando il costo della protezione supera il danno potenziale; decisione basata sull'attitudine al rischio dell'azienda
- **Transfer**: Spostare l'impatto su un terzo
  - Esternalizzare processi critici a fornitori Cloud che offrono garanzie contrattuali (SLA)
  - **Assicurarsi…**

Rischio residuo

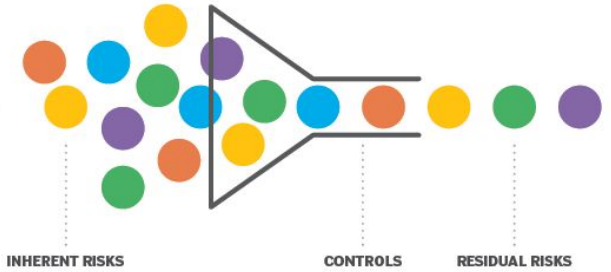
https://www.techtarget.com/searchsecurity/definition/residual-risk

- È quella parte di pericolo che rimane dopo aver definito la propria strategia di gestione
- È l'evento "catastrofico" o l'errore umano difficile da prevedere

Il rischio residuo deve essere **quantificato** per quantificare la **copertura assicurativa** serve

Parziale perdita del controllo dei propri dati, da valutare attentamente nell'attuale contesto geopolitico

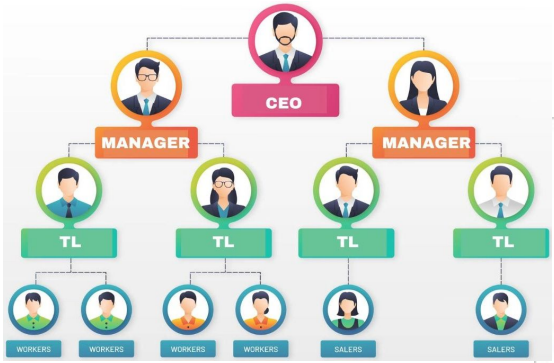
Il ruolo dell'assicurazione



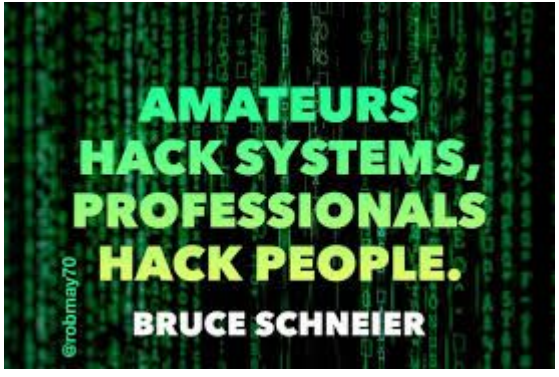
- **Protezione bilancio**: trasforma un costo potenziale enorme e improvviso in un premio assicurativo certo e pianificato
- **Supporto specialistico**: le polizze non forniscono solo copertura finanziaria, ma anche una "task force" di esperti (legali, tecnici, PR) dopo un attacco
- **Accesso al credito e supply chain**: essere assicurati dimostra ai partner e alle banche che l'azienda è gestita con criteri di maturità manageriale

- L'assicurazione non è un'alternativa alle difese ma il completamento della strategia di gestione del rischio
- Nessun assicuratore copre un'azienda senza una strategia matura di gestione del rischio

Il ruolo della NIS2

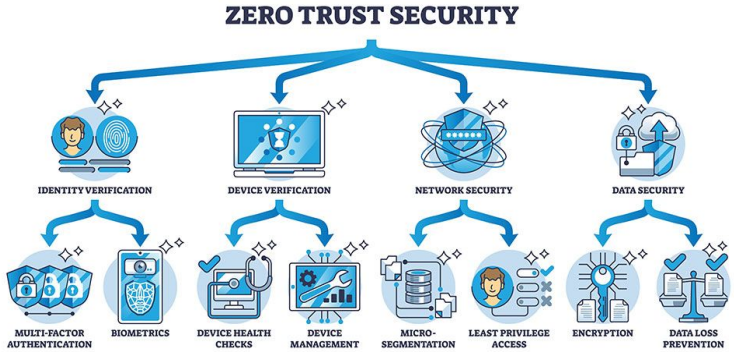


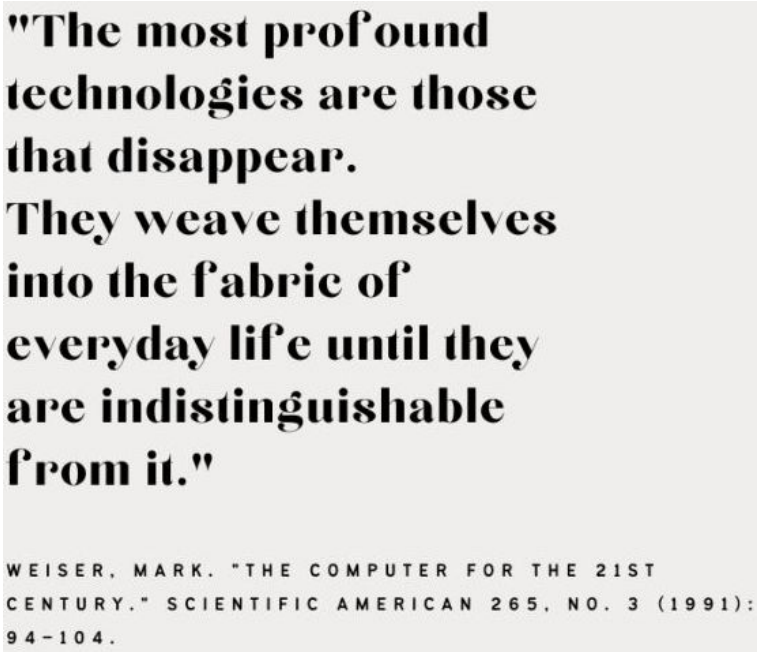
- Sposta il baricentro della cybersecurity da ambito tecnico a gestionale
- **Responsabilità del management**: la governance del rischio cyber ricade direttamente sul CDA, rendendo la sicurezza una priorità di vertice
- **Focus sulla disponibilità**: impone la business continuity
  - Proteggere il dato significa garantirne la disponibilità per la produzione
- **Cultura e fattore umano**: formazione
  - Investire nella consapevolezza dei dipendenti trasforma il personale da "punto debole" a “prima linea di difesa” contro social engineering (es. phishing)
- **Sicurezza della supply chain**: la conformità alla NIS2 diventa un requisito commerciale per restare fornitori di grandi gruppi industriali



Non dimentichiamo le basi*!*

- Identità digitale
  - Non solo per gli utenti ma anche per dispositivi, processi ed agenti AI*!*
  - Base di partenza per altri controlli di sicurezza e **tracciabilità**
  - Zero Trust: **fidati ma verifica** (ad ogni accesso)
- Evoluzione del concetto di “superficie d’attacco”
  - Zero Trust: **segmentazione** e **controllo degli accessi** (delega e principio “least privilege”)
  - **AI pen testing**: Mythos (hype?) e cambio gestione CVE (+263% nel periodo 2020-2025)
  - Nessuna azienda è un’isola ma è inserita in un ecosistema complesso (**supply chain**)
- Minimizzare “sovraccarico” sugli utenti dovuto alla sicurezza
  - Esperienza utente “**senza**” **frizioni**
  - Le tecnologie di **maggiore successo** sono quelle che… **spariscono**
- Cultura aziendale
  - Costruire **consapevolezza** dei rischi a tutti i livelli (AD, CdA, …)
  - Focus su **Social Engineering** e **Deep fake**

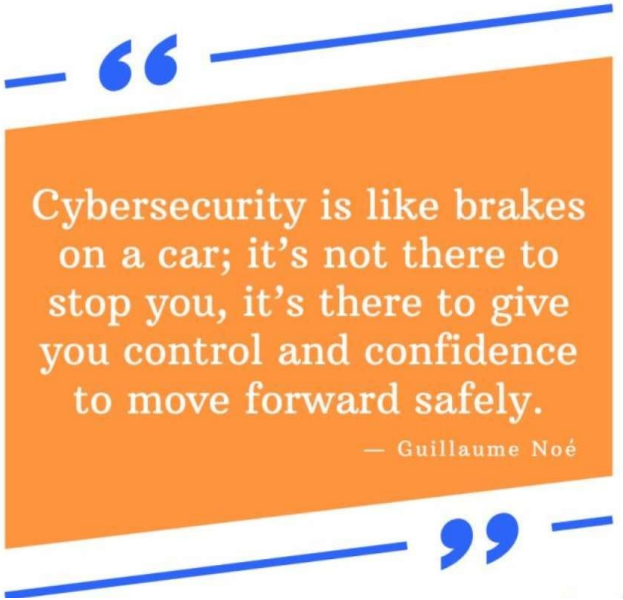




Punti chiave

Un possibile approccio alla gestione integrata dei rischi di sicurezza

- Calcolare RTO
  - In quanto tempo si riparte in caso di arresto?
- Valutare il rischio residuo ed il suo trasferimento:
  - identificare cosa non si può proteggere
  - valutare una copertura assicurativa cyber
- Usare la NIS2 come guida
  - implementate i requisiti non per obbligo, ma per resilienza



Considerate la cybersecurity non come un problema da risolvere, ma un rischio da gestire per proteggere il futuro dell'impresa