Deloitte.

Deloitte Consulting S.r.l. S.B.- Cyber

Cybersecurity Impegni, Sfide e Opportunità per le Imprese

Cuneo, 29 Gennaio 2025

Lo speaker

Lorenzo Russo
Partner | Deloitte Risk Advisory

lorusso@deloitte.it

Bio

Partner di Deloitte Risk Advisory con esperienza di oltre 25 anni in ambito Cyber Security Strategy, Governance & Risk Management, maturata in progetti con governi, organizzazioni internazionali e aziende Fortune 500. Co-autore del Framework Nazionale per la Cyber Security e del NATO Next Generation CERTs Handbook e Advisor delle UN per temi di National Cyber Strategy e Capacity Building

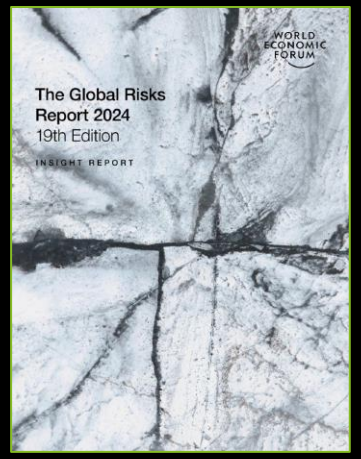
Percezione e Realtà del Rischio Cyber

Percezione del Rischio Cyber a Livello Globale – WEF Global Risks Report 2025

Il World Economic Forum (WEF) conferma il rischio Cyber fra i principali rischi percepiti dalle organizzazioni mondiali per i prossimi due anni, evidenziandone la rilevanza in un contesto di crisi e trasformazioni globali

WEF Global Risk Report 2024

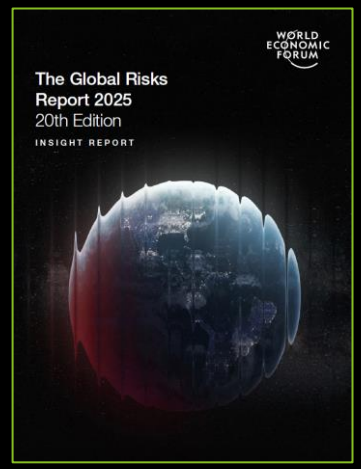
Top 10 Rischi Globali Percepiti per i Prossimi 2 anni



1. Misinformation and disinformation
2. Extreme weather events
3. Societal polarization
4. Cyber insecurity
5. Interstate armed conflict
6. Lack of economic opportunity
7. Inflation
8. Involuntary migration
9. Economic downturn
10. Pollution

WEF Global Risk Report 2025

Top 10 Rischi Globali Percepiti per i Prossimi 2 anni



1. Misinformation and disinformation
2. Extreme weather events
3. State-based armed conflict
4. Societal polarization
5. Cyber espionage and warfare
6. Pollution
7. Inequality
8. Involuntary migration or dispiacement
9. Geoeconomic confrontation
10. Erosion of human rights &/or civic freedoms

Legenda Categoria Rischi

Economico · Ambientale · Geopolitico · Sociale · Tecnologico

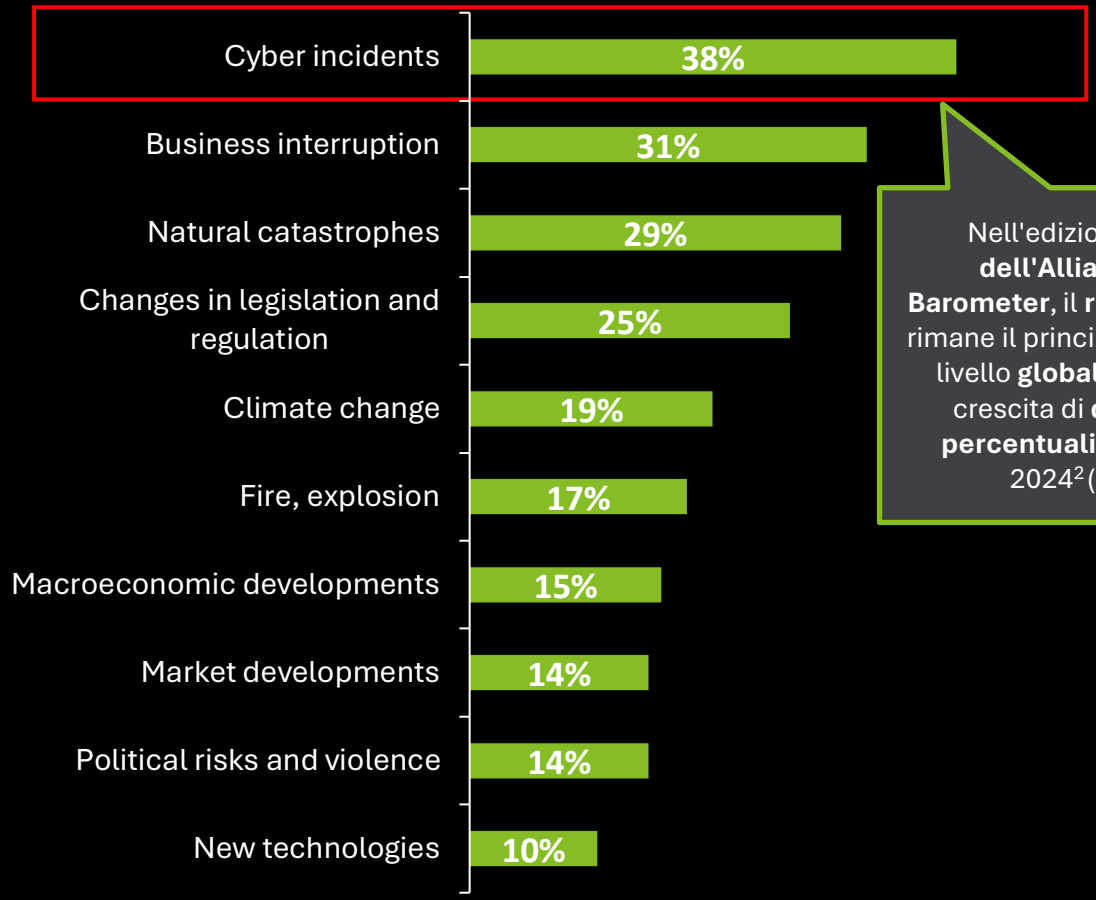
Fonte: WEF Global Risk Report, 2024 e 2025

Percezione del Rischio Cyber a Livello Globale e Italiano – Allianz Risk Barometer 2025

Nell'edizione 2025 dell'Allianz Risk Barometer, le aziende a livello globale identificano il rischio Cyber come il principale rischio percepito per il proprio Business. Questa tendenza è confermata anche in Italia, dove il rischio Cyber si colloca al primo posto tra le preoccupazioni più rilevanti per le imprese

Allianz Risk Barometer 2025

Top 10 Rischi Percepiti dalle Aziende nel Mondo[1]



Nell'edizione **2025 dell'Allianz Risk Barometer**, il **rischio Cyber** rimane il principale rischio a livello **globale,** con una crescita di **due punti percentuali** rispetto al 2024[2] (36%)

Top 3 Rischi Percepiti in l'Italia

1. Cyber Incidents

2. Natural catastrophes

3. Business Interruptions

Nota: 1) Il numero di rischi selezionati è rappresentato come percentuale di tutte le risposte al sondaggio da parte di 3.778 intervistati. Ogni partecipante poteva scegliere fino a tre rischi per settore, motivo per cui i valori non sommano al 100%; 2) Rispetto all'Allianz Risk Barometer 2024

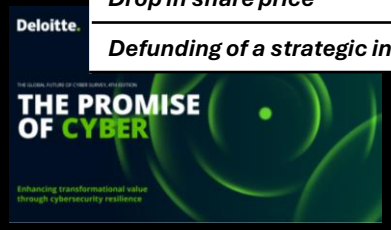
Percezione del Rischio Cyber a Livello Globale – Survey Deloitte 2024

Secondo la 4ª edizione della Global Future of Cyber Survey di Deloitte, la Cyber Security sta acquisendo un ruolo sempre più rilevante nel potenziare il valore strategico delle aziende, diventando una componente fondamentale per il raggiungimento degli obiettivi aziendali

Le principali conseguenze degli incidenti Cyber secondo le aziende

Principali conseguenze degli incidenti Cyber secondo le aziende	3° Edition (Rank)	3° Edition (Percent)	4° Edition (%)	4° Edition (%)
Loss of confidence in tech integrity	6	55%	1	66%
Operational disruption (including supply chain/or partner ecosystem)	1	58%	2	66%
Reputational loss	4	55%	3	65%
Negative talent recruitment/ retention impact	7	54%	4	64%
Loss of revenue	2	56%	5	64%
Loss of customer trust/negative brand impact	3	56%	6	63%
Intellectual property theft	8	54%	7	63%
Regulatory fines	10	52%	8	63%
Drop in share price	9	52%	9	63%
Defunding of a strategic initiative	5	55%	10	63%

Per la maggior parte delle organizzazioni, i principali **impatti negativi** derivanti da un **incidente Cyber** sono l'**interruzione** dell'**operatività** aziendale e la **perdita** di **fiducia** nella **sicurezza intrinseca della tecnologia**



Benefici strategici degli investimenti in Cyber Security

Fonte: Deloitte - 4ª edizione della Global Future of Cyber Survey, 2024

I Presidi per la Gestione del Rischio Cyber

Presidi per una Gestione Efficace del Rischio Cyber

Le aziende devono adottare un approccio strutturato per la gestione della Cyber Security che includa specifici presidi di controllo, anche in coerenza con le nuove normative in materia

Presidi	Attività
Risk Ownership	Il **Top Management** deve svolgere un **ruolo attivo** nella **gestione** dei **rischi**, in particolare nella definizione di una **strategia** di gestione del rischio Cyber e nella promozione di formazione in ambito cyber security con l'obiettivo di migliorare la sicurezza e resilienza informatica
Modello di Governance	L'azienda deve **definire** e adottare un **modello** di **governo** della Cyber Security, che preveda una chiara attribuzione di ruoli e responsabilità ai diversi **Stakeholder** aziendali, a tutela dei diversi ambiti da salvaguardare: IT, OT, IoT, con modalità di controllo ben strutturate
Misure di Gestione Rischio Cyber	L'azienda deve implementare misure **tecniche**, **organizzative** e **procedurali** adeguate e proporzionate, garantendo una protezione efficace e continua dei **sistemi IT** e **OT e IoT**
Sicurezza della Supply Chain	Deve essere sviluppato un **processo** di **gestione** del **rischio** lungo la Supply Chain che preveda specifici **presidi** di Cyber Security, come la definizione di **clausole contrattuali** e la valutazione della **postura** di **sicurezza** dei **fornitori** prima e dopo la contrattualizzazione
Gestione degli Incidenti	L'azienda deve dotarsi di tecnologie, processi e competenze per effettuare un'adeguata **gestione** degli **incidenti** di sicurezza in modo da assicurare un'efficace **risposta** e **mitigazione** degli **impatti**, garantendo il **ripristino** della normale operatività

Focus: Risk Ownership

Il Top Management deve avere un ruolo di responsabilità nella gestione dei rischi Cyber e deve promuovere e partecipare ad iniziative di formazione in ambito

Principali Responsabilità del Top Management

Definizione di strategie di Gestione del Rischio Cyber

Approvazione e supervisione delle misure di gestione del rischio Cyber

Partecipazione a programmi di formazione in ambito Cyber e promozione di attività di Training periodico ai propri dipendenti

Una delle principali **sfide** per le aziende è rappresentata dall'integrazione del **Chief Information Security Officer** (CISO) in un **ruolo** sempre più **strategico**. Circa un terzo delle organizzazioni evidenzia un **incremento significativo** della sua **partecipazione** nelle discussioni su **tecnologie chiave** (e.g. Cloud, Intelligenza Artificiale, 5G, etc.)[1]

1) Fonte: Deloitte - 4ª edizione della Global Future of Cyber Survey, 2024

Focus: Modello di Governance

È fondamentale sviluppare un Modello di Governo della Cyber Security che garantisca l'identificazione degli Stakeholder aziendali coinvolti e la definizione e assegnazione di specifici ruoli e responsabilità

Approccio per la predisposizione del Modello di Governo

1 Identificazione Macro-attività

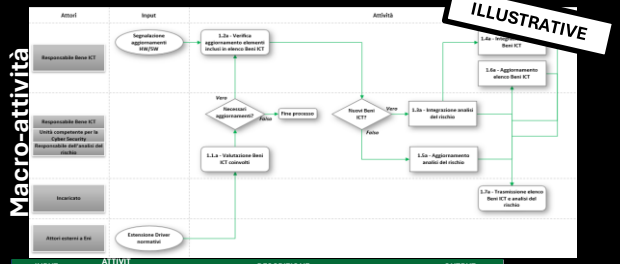
Identificazione delle **attività** chiave, sulla base degli **ambiti** di **Gestione del Rischio Cyber**

- **Risk Ownership**
- **Misure di Gestione del Rischio Cyber**
- **Sicurezza della Supply Chain**
- **Gestione degli Incidenti**

2 Definizione Ruoli e Responsabilità

Identificazione degli **Stakeholder** coinvolti e **predisposizione** dei **Workflow** per formalizzare **ruoli, responsabilità** e **modalità** di **interazione**

Workflow Macro-attività



Dettaglio Attività

Tabella RACI

ATTIVITA'	R	A	C	I
1.1a - Valutazione Asset coinvolti	Responsabile Servizio/Funzione Essenziale	Incaricato	Responsabile Business Cyber Sec Compliance	-
1.2a - Verifica aggiornamento elementi inclusi in elenco beni ICT	Responsabile Servizio/Funzione Essenziale	Incaricato	Cyber Sec Compliance	-
1.3a - Integrazione analisi del rischio	Responsabile Servizio/Funzione Essenziale	Incaricato	Cyber Sec Responsabile Business	-
1.4a - Integrazione elenco beni ICT	Responsabile Servizio/Funzione Essenziale	Incaricato	Cyber Sec	-
1.5a - Aggiornamento analisi del rischio	Responsabile Servizio/Funzione Essenziale	Incaricato	Cyber Sec Responsabile Business	-
1.6a - Aggiornamento elenco beni ICT	Responsabile Servizio/Funzione Essenziale	Incaricato	Cyber Sec	-
1.7a - Trasmissione elenco beni ICT e analisi del rischio	Incaricato	Incaricato	-	Cyber Sec Responsabile Business Responsabile Servizio/Funzione Essenziale

3 Definizione Modello di Governo

Definizione del Modello di Governo comprensivo di **flussi, processi** e **attività** che **coinvolgono** gli **Stakeholder aziendali**

Focus: Misure di Gestione del Rischio Cyber

Al fine di garantire un'adeguata gestione del rischio Cyber, le aziende dovrebbero definire e attuare una serie di misure di sicurezza chiave adeguandosi alle principali Best Practice e Standard di settore

Misure di Gestione del Rischio Cyber

- Policy di **Cyber Security** e di **gestione dei rischi**
- Gestione degli **incidenti**
- **Business Continuity** e **Disaster Recovery**
- **Sicurezza** della **catena** di **approvvigionamento** (Supply Chain)
- Programmi di **Training** & **Awareness** su rischio Cyber
- Gestione delle **vulnerabilità**
- Sicurezza dell'**acquisizione**, dello **sviluppo** e della **manutenzione** dei **sistemi informatici** e di **rete**
- Utilizzo di tecniche di **crittografia** e **cifratura** per la **protezione** dei **dati**
- Soluzioni di **gestione** e **protezione** degli **accessi** alle risorse aziendali
- Modalità di **accesso** e **autenticazione** sicure (es. MFA, ...)

Focus: Sicurezza della Supply Chain 1/2

Al fine di garantire la sicurezza della Supply Chain deve essere definito un processo per la gestione del rischio Cyber che integri specifici presidi dalla fase di qualifica fino alla gestione contrattuale

ILLUSTRATIVE

Fasi del Processo

Processi

Qualifica	Pre-Award	Post-Award
▪ Definizione di **cluster** di **Gruppi Merce** con differenti livelli di **rischio Cyber** ▪ Verifica della **Cyber Posture** dei fornitori tramite **analisi Risk-Based** in funzione della criticità Cyber del Gruppo Merce sul quale intendono qualificarsi	▪ Definizione di una **metodologia** a supporto dell'unità richiedente per identificare il **rischio Cyber** associato ad ogni **fornitura** ▪ Definizione di un **processo** e di una **checklist** utili ad effettuare la **valutazione** Cyber del fornitore ▪ Definizione di **Clausole standard** per contratti a rischio Cyber	▪ Definizione di una **metodologia** Risk-Based per il **monitoraggio** dei contratti

Persone

- **Valutazione di Cyber Security** dei fornitori durante **le fasi del processo di approvvigionamento**
- Esecuzione di **iniziative** utili a **sensibilizzare** e responsabilizzare le **Terze Parti** in materia di Cyber Security
- Definizione di un **modello operativo** e **organizzativo** sostenibile che riduca il **rischio** di **Cyber Security**

Technologie

- Identificazione e implementazione di **strumenti** di **automazione** dei processi per facilitare l'interazione tra Stakeholder (es. Cyber Security, Procurement, Contract Manager, etc.)
- Identificazione di **servizi/soluzioni** in grado di fornire informazioni sulla **Cyber Security Posture** dei **fornitori** (es. Security Rating Services)

Focus: Gestione degli Incidenti

Per una gestione tempestiva ed efficace degli incidenti Cyber, è necessario definire un processo caratterizzato da differenti fasi, garantendo una comunicazione costante e un coordinamento tra tutti gli Stakeholder interessati

1

- **Rilevamento** degli **incidenti** attraverso la condivisione delle informazioni, notifiche dagli utenti, analisi degli eventi tramite i sistemi di sicurezza / SOC / OSINT
- Sviluppo di **indicatori** e **specifiche metriche** per il rilevamento tempestivo degli incidenti

2

- **Analisi** e **classificazione** degli **incidenti**, raccolta, correlazione e analisi approfondita delle evidenze degli stessi
- **Triage** e **attivazione del processo** di **risposta** agli incidenti e agli impatti correlati
- **Definizione** delle **misure** di **escalation** per rispondere tempestivamente agli incidenti

3

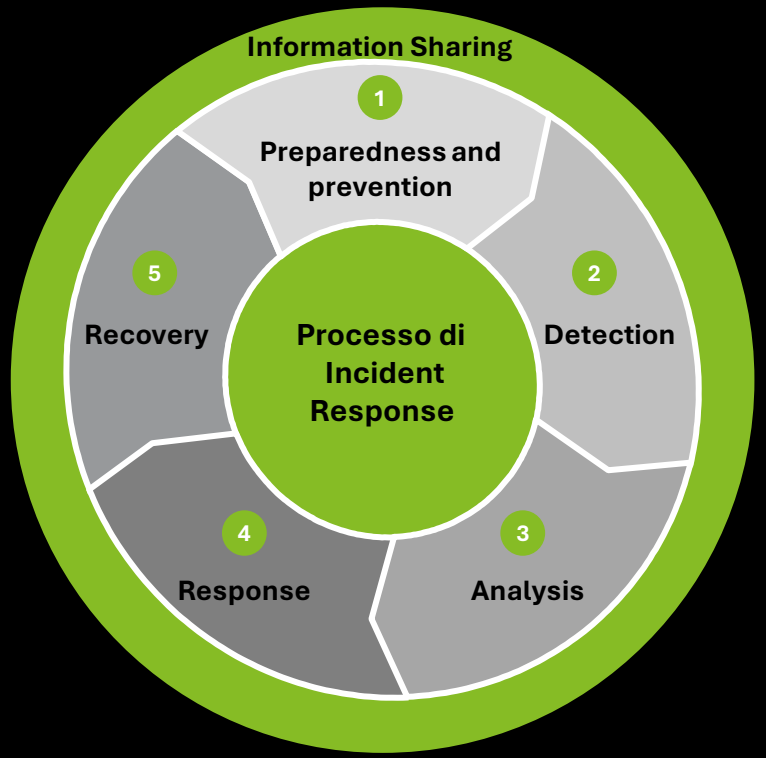
- Attività di **supporto** alla **risposta**
- **Comunicazione** verso gli Stakeholder rilevanti tramite canali resilienti o standard, a seconda degli Stakeholder interessati
- **Coordinamento** e **cooperazione** con la Costituency e gli Stakeholder

4

- **Identificazione** delle **misure** volte a ripristinare i servizi una volta neutralizzata la minaccia
- **Progettazione** del **Recovery Plan**, comprese le risorse necessarie per ripristinare i livelli di servizio standard
- **Miglioramento** della **Baseline** di **conoscenze** tramite la definizione e la condivisione delle lesson learned

5

- **Redazione** delle **regole** della **Costituency** sulla **Cyber Security** basate su standard nazionali e internazionali, best practices, lesson learned
- **Supporto** e **monitoraggio** della **Costituency** implementando un insieme di controlli basati su linee guida
- Attività di **disseminazione**



Deloitte.

MAKING AN IMPACT THAT MATTERS since 1845