

# 19° FORUM RISK MANAGEMENT AREZZO

## IL MODELLO DI HEALTHCARE ENTERPRISE RISK MANAGEMENT

# AON GLOBAL RISK CONSULTING

Aon Global Risk Consulting (AGRC) è l'organizzazione globale del Gruppo Aon dedicata alla consulenza strategica di risk management

**AGRC nel mondo....**

- Presente in **50 paesi**
- + 2.000 Risk Professionals**

**...e in Italia**

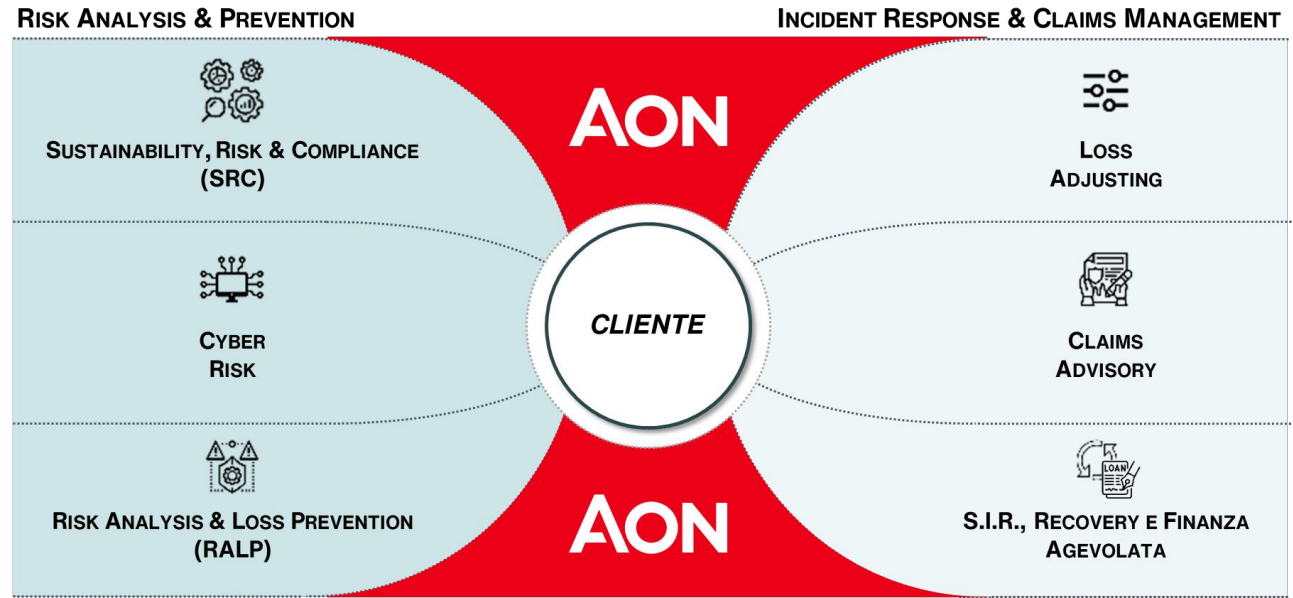
- 600+** Progetti di consulenza (ultimi 2 anni)
- 80+** Partnership R&D internazionali (ultimi 2 anni)



**Enrico Trombetta**  
**Deputy Head of Consulting for Italy and South-East Europe di Aon**

È specializzato nell'implementazione di Modelli di Gestione del Rischio, sia a livello Enterprise che verticali, e nella consulenza strategica in ambito ESG & Sustainability. Ha una vasta esperienza in Data Analytics, Supply Chain Risk Analysis, Fraud Detection, implementazione di Dashboard di monitoraggio continuo ed automatizzato dei processi.

## Le soluzioni di Aon Global Risk Consulting (AGRC) Italia



# HERM REGIONE LOMBARDIA – OVERVIEW

Il progetto nasce dalla forte volontà della **DG Welfare** e del **Centro Regionale per la Gestione del Rischio Sanitario** e la **Sicurezza del Paziente** di far **evolvere il modello di Risk Management** verso una **gestione integrata dei rischi**.

È stato oggetto di uno Decreto attuativo (Decreto n. 20638 del 21/12/2023 c.d. «**Decreto HERM**») e di pubblicazione su Pubmed (The **ERM experience of the Lombardy Region**)

**Healthcare**

**Enterprise Risk Management**



Linee di riferimento per  
 l'implementazione dell'Healthcare  
 Enterprise Risk Management  
 (HERM) nel sistema socio-sanitario  
 regionale

PubMed®

The ERM experience of the Lombardy Region as a tool for improving the safety of the regional health care system

Enrico Burato<sup>1</sup>, Liviana Scotti<sup>1</sup>, Enrico Trombetta<sup>1</sup>, Giacomo Taddei<sup>1</sup>, Alessandro Audino<sup>1</sup>, Enrico Malinverno<sup>1</sup>, Davide Molteni<sup>1</sup>, Giorgia Saporetti<sup>1</sup>, Alessandra Rossodivita<sup>1</sup>, Silvana Castaldi<sup>1</sup>, Rossella Barni<sup>1</sup>, Simona Amato<sup>1</sup>

Affiliations + expand  
 PMID: 38112037

**Abstract**

The Regional Center for Healthcare Risk Management and Patient Safety of the Lombardy Region, with the technical partnership of Aon, designed an innovative Healthcare Enterprise Risk Management Model (hereafter HERM) to meet the following objectives: 1) Improve the safety of the Regional Healthcare System through the implementation of methods and tools aimed to identify, analyze and manage in an integrated way all the risks to which are exposed the healthcare companies. 2) Preserve the creation of social value in the medium-long term and the sustainable achievement of strategic and operational objectives. 3) Optimize risk management costs. 4) Reduce/mitigate adverse events in all business processes. 5) Enable the ability to anticipate and react to changes. 6) Establish sound long-term and risk-based strategies. This paper describes the structuring of the overall HERM Model Framework, and the related information flows, the tools supporting the Healthcare Enterprise Risk Management Methodology (such as the Risk Model and the Assessment Metrics) and presents the preliminary result of first experience of Healthcare ERM in Italy.



# HERM – IL RISK MANAGEMENT PROCESS

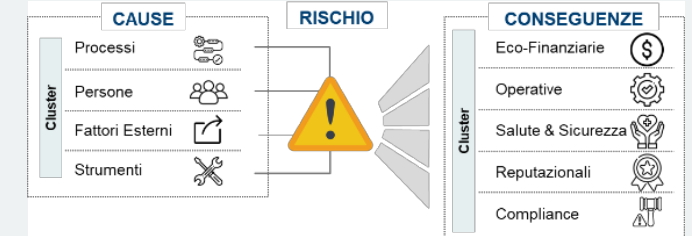
## ATTIVITÀ

## DELIVERABLE (Esemplificativi)



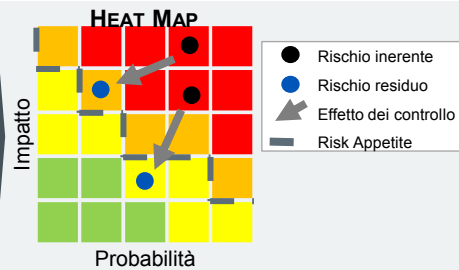
- **Analisi** della **documentazione** aziendale (es. policy, procedure, etc.);
- **Risk Universe** della **Industry**; Studi di settore/Aon expert opinion;
- **Interviste** con il **management aziendale**.

Invio documenti e interviste



- Valutazione di **Rischio Inerente e Residuo**, assegnando uno **score** a:
  - **probabilità** di accadimento;
  - **massimo danno** verificabile, considerando gli effetti diretti e indiretti;
  - tipologia di **controllo** (preventivo o correttivo)<sup>1</sup>.
- **Classificazione** dei rischi rispetto al **Risk Appetite**<sup>2</sup> aziendale

Risk Appetite

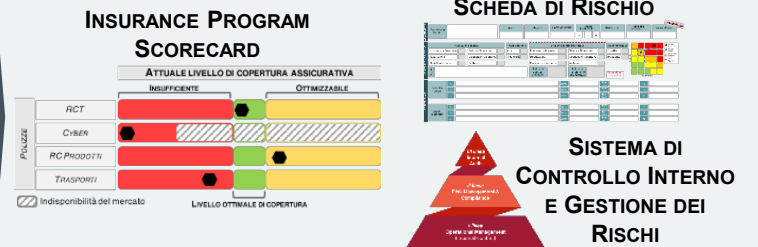


- <sup>1</sup> **Tipologia di controlli:**
- **Preventivi:** riducono la probabilità di accadimento
  - **Correttivi:** riducono l'impatto (intervengono dopo il verificarsi dell'evento)



- **Identificazione** di:
  - **azioni di mitigazione** operative e organizzative;
  - **strategie assicurative** per ottimizzare le polizze rispetto al profilo di rischio
- Per ciascun Top Risk, predisposizione della **Scheda di Rischio** corredata dall'Action Plan (ownership, due date e stima investimenti);
- **Valutazione** del livello di maturità delle tre linee di difesa del **Sistema di Controllo Interno e Gestione dei Rischi (SCIGR)**

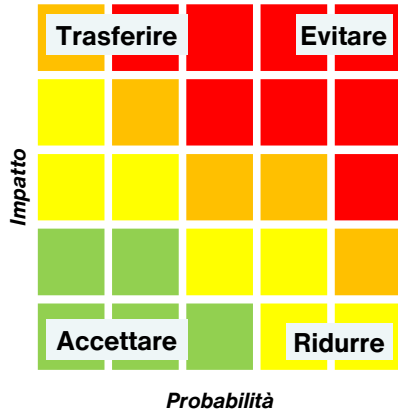
Scheda di Rischio



(2) Massimo livello di rischio accettabile per l'azienda, definito nelle fasi iniziali di progetto.

# HERM – TREATMENT STRATEGY SETTING

Strategie di gestione del rischio



Accettare	Evitare	Ridurre	Trasferire		
Non si adottano azioni di alcun tipo per ridurre l'esposizione al rischio.	Si intraprendono azioni per eliminare alla radice le cause di esposizione al rischio.	Si adottano azioni per calmierare l'esposizione al rischio (misure preventive e correttive)	Si intraprendono azioni di <b>trasferimento del rischio</b> in tutto o in parte a terzi (es. mediante assicurazione o revisione contratti con terze parti).		
Misure integrate di gestione del rischio	STRATEGICHE	ORGANIZZATIVE	OPERATIVE	ASSICURATIVE	CONTRATTUALI

Strumenti Aon

### MATRICE DI PRIORITIZZAZIONE DELLE AZIONI

Strumento utilizzato per prioritizzare le azioni sulla base del relativo livello di efficacia e della complessità di esecuzione (effort).

Efficacia	Alta	Azioni a priorità 2	Azioni a priorità 1 <b>Quick Win</b>
	Bassa	Non implementare	Azioni a priorità 3
		Ridotta	Elevata
		Facilità Realizzativa	

### INSURANCE PROGRAM SCORECARD

Strumento grafico utilizzato per rappresentare i gap di natura assicurativa e per individuare quali coperture estendere e quali ottimizzare.

*Esemplificativo*

		ATTUALE LIVELLO DI COPERTURA ASSICURATIVA	
		INSUFFICIENTE	OTTIMIZZABILE
POLIZZE	RCT/O	[Red bar]	[Yellow bar]
	CYBER	[Red bar with gap]	[Yellow bar with gap]
	PROPERTY	[Red bar]	[Yellow bar]
	TRASPORTI	[Red bar]	[Yellow bar]
		Indisponibilità del mercato	LIVELLO OTTIMALE DI COPERTURA



# HERM REGIONE LOMBARDIA – PRINCIPALI AREE DI RISCHIO

ALCUNE DELLE PRINCIPALI AREE DI RISCHIO



Attacchi cyber

FOCUS NELLE  
PROSSIME SLIDE



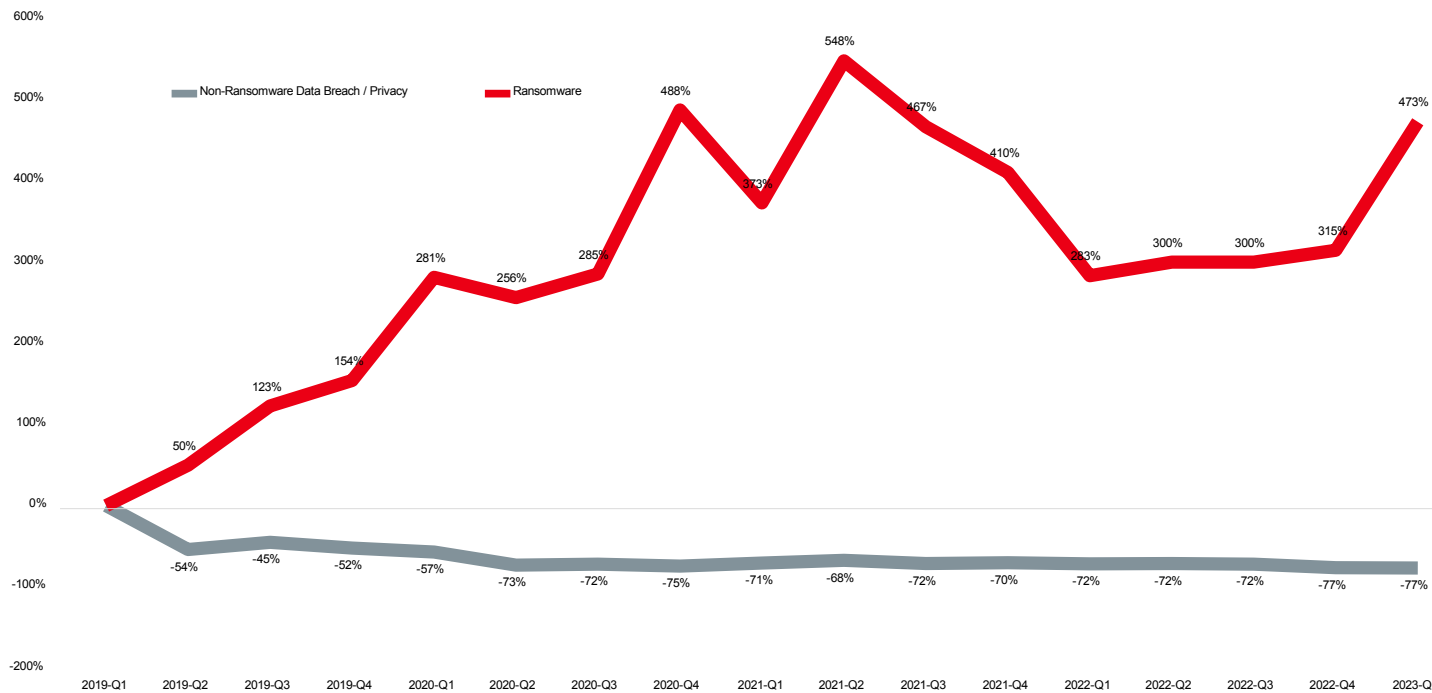
- Individuate **azioni di mitigazione**;
- Definiti piani di **monitoraggio dell'implementazione** delle azioni di mitigazione;
- Definiti piani di **audit risk-based**.

Inoltre, nell'ultimo anno si è verificato un incremento dei valori medi dei sinistri di responsabilità sanitaria, con maggiore pressione sulle risorse economico-finanziarie del Sistema Sanitario.

FOCUS NELLE  
PROSSIME SLIDE

# RISCHIO CYBER – UN TREND IN CRESCITA

Tasso degli incidenti informatici nel periodo Q1 2019 – Q1 2023



Source:

1. Risk Based Security, analysis by Aon. Data as of 03/04/2023
2. Rapporto Clusit 2023 (ed. Marzo 2023)

Dopo una lieve riduzione nella frequenza dei cyber claim durante il 2022, i primi mesi del 2023 tornano a registrare un aumento importante nel numero di attacchi ransomware toccando i livelli del periodo pandemico (2020 – 2021).

Ad essere peggiorata è oltretutto la severità degli attacchi con ripercussioni sempre più gravi.

## Osservazioni chiave:

- La **frequenza** degli **attacchi ransomware** ha superato in modo stabile la frequenza degli eventi di Data e Privacy Breach non correlati ad attività di ransomware
- **Nel Q1 2023 gli attacchi ransomware noti sono a +473% rispetto al medesimo trimestre del 2019**
- Oltre alla frequenza è anche drasticamente peggiorata la **severità** degli attacchi che risultano ora avere **conseguenze decisamente più impattanti**
- I settori più colpiti da attacchi ransomware al Q1 2023 sono stati il settore manifatturiero, dell'istruzione, finanziario, sanitario e della pubblica amministrazione
- Secondo il Rapporto Clusit 2023 l'Italia sembra essere nel «mirino» dei cyber criminali ricevendo il 7,6% degli attacchi globali



# RISCHIO CYBER – LA DIRETTIVA NIS2

La **Direttiva sulla sicurezza delle reti e delle informazioni NIS2** (Network and Information Security) è entrata a gennaio 2023 e introduce nuovi obblighi di cybersicurezza per la Pubblica Amministrazione e le grandi e medie imprese

## Perimetro e Sanzioni:

La Direttiva si applica anche ai soggetti che operano in **ambito Sanità** (compresi la fabbricazione di prodotti farmaceutici e i vaccini), con riferimento a:

### Soggetti Importanti

Medie organizzazioni con

**50-250 dipendenti e fatturato > 10 mln€**

Sanzioni **fino a 7mln€** o almeno l'**1,4% del totale del fatturato annuo**

### Soggetti Essenziali

Grandi organizzazioni con

**+250 dipendenti e fatturato > 50 mln€**

Sanzioni **fino a 10mln€** o almeno il **2% del totale del fatturato annuo**

## Roadmap:

entro il 31/01/2024	Valutazione <b>applicabilità NIS2</b>
entro il 28/02/2025	Registrazione su <b>piattaforma ACN<sup>2</sup></b>
entro il 15/04/2025	Nomina <b>responsabile fornitura informazioni</b>
dal 1/01/2026	Inizio <b>obbligo notifica incidenti</b>
entro il 1/10/2026	Adempimento <b>altri obblighi</b>

## Obblighi:

### Misure di gestione dei rischi di cybersicurezza

Adozione di misure tecniche, operative e organizzative, quali:

- Cyber Risk Analysis
- Business Continuity
- Monitoraggio Supply Chain
- Multi-Factor Authentication

### Governance dei rischi di cybersicurezza

Gli organi di gestione sono tenuti ad adeguarsi alla normativa e a:

- individuare i rischi
- valutare le pratiche di gestione dei rischi
- seguire una formazione specifica (anche per i dipendenti)

### Obblighi di segnalazione degli incidenti

Segnalazione degli incidenti al CSIRT<sup>1</sup> o ad altre autorità:

- **entro 24 ore** da quando sono venuti a conoscenza dell'incidente, **preallarme**;
- **entro 72 ore**, **notifica** aggiornata dell'incidente
- **entro un mese**, **relazione finale** dell'incidente



# OSSERVATORIO AON SUI SINISTRI HEALTHCARE

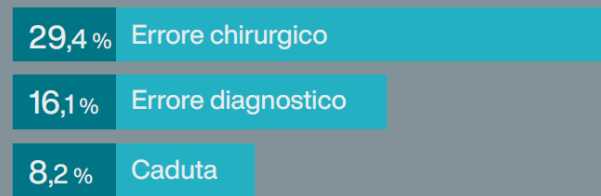
L'Osservatorio, focalizzato sull'analisi dei sinistri nel corso di un decennio, offre una visione del rischio nel settore tra le più ampie in Italia.



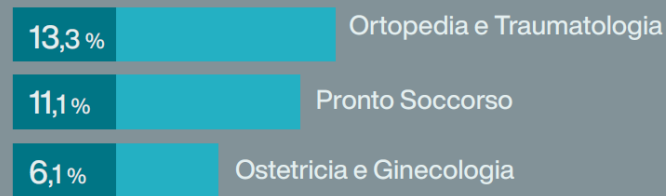
**Utilità per le strutture sanitarie**

Confronto e posizionamento del proprio andamento con i dati medi di riferimento presenti nell'Osservatorio Aon Rischi in Sanità – Healthcare Claims Trends

## Principali Eventi

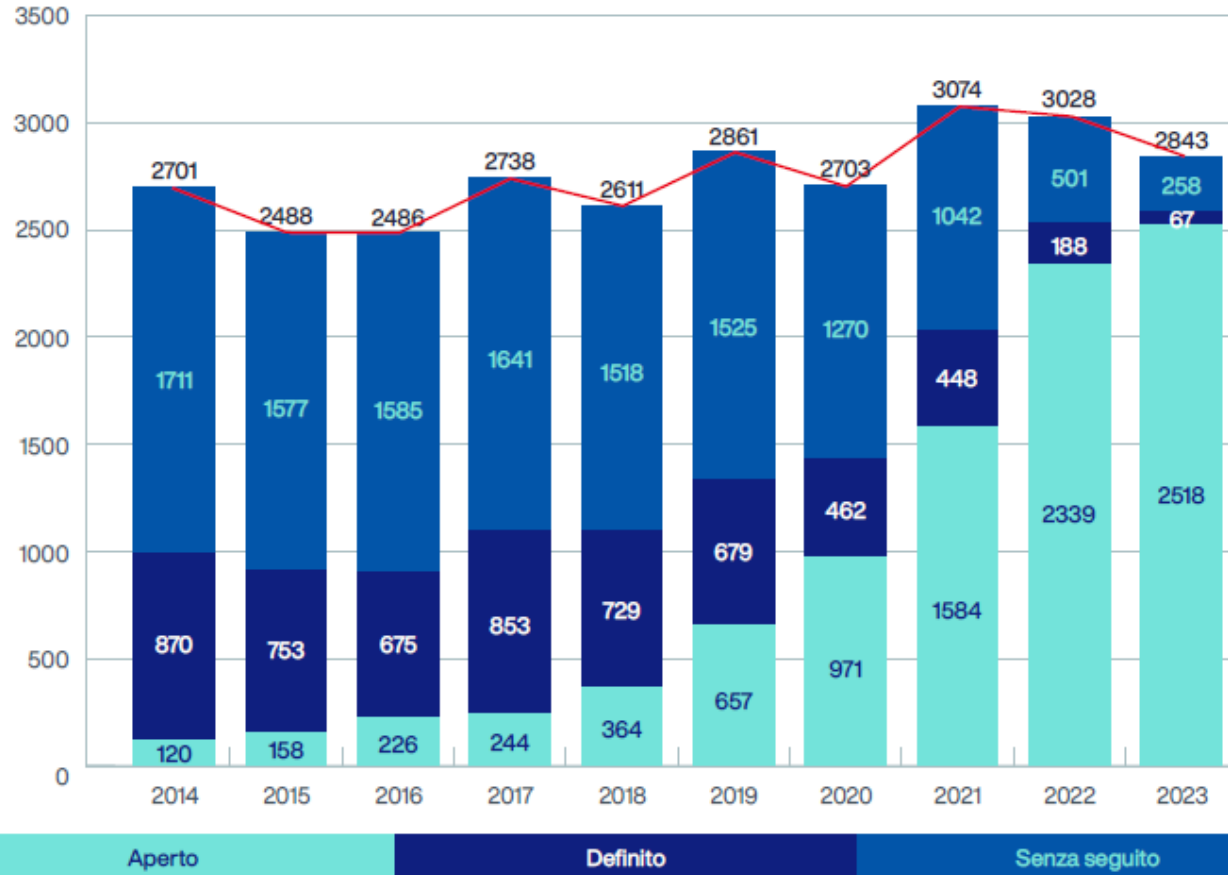


## Principali Specialità





# OSSERVATORIO AON SUI SINISTRI HEALTHCARE – EVIDENZE



L'andamento dei sinistri mostra come il **2021** abbia rappresentato l'anno di **picco** in termini di numerosità dei sinistri, registrando un totale di 3.074 sinistri.

Successivamente, si osserva un trend in **flessione negli anni 2022 e 2023** con una riduzione complessiva del **7,5%**.

Tuttavia, nell'ultimo anno si è verificato un **incremento dei valori medi dei sinistri di responsabilità sanitaria**, con maggiore pressione sulle risorse economico-finanziarie del Sistema Sanitario.

# TAKE HOME

## TAKE HOME



Il Modello di **Healthcare Enterprise Risk Management** è una **best practice** in ambito Sanità e consente di **ottimizzare la spesa** per la mitigazione dei rischi

---



Il **rischio Cyber** è uno dei **principali rischi in ambito Sanità**: Aon può dare supporto nella gestione di tale rischio e nell'adeguamento alle nuove normative come la NIS2

---



Nell'ultimo anno si è verificato un **incremento dei valori medi dei sinistri di responsabilità sanitaria**: dotarsi di un buon **programma assicurativo** è un fattore critico di successo

## CONTATTI

**Enrico Trombetta**

Deputy Head of Consulting – Italy & South-East Europe

[enrico.trombetta@aon.it](mailto:enrico.trombetta@aon.it)

Mobile: +39 335 8016078

