



Ransomware

Un attacco ransomware causa danni devastanti a qualsiasi organizzazione in quanto viene compromessa:

- l'integrità dei dati (che vengono cifrati dal ransomware)
- la disponibilità di uno o più servizi
- la riservatezza dei dati (se oltre alla cifratura c'è stata una esfiltrazione degli stessi)

Ad oggi le gang criminali sono arrivati ad utilizzare fino a 4 tipologie di estorsione:

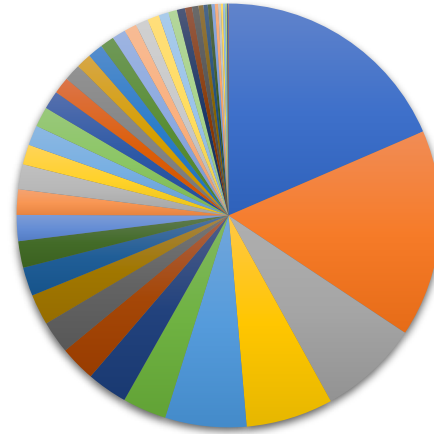
1. Cifratura dei dati
2. Pubblicazione dei dati
3. Attacco DDoS
4. Minacce ai contatti

Analisi completa

<https://www.cybersecurity360.it/nuove-minacce/ransomware/ransomware-che-ce-da-sapere-per-adottare-una-corretta-strategia-difensiva-nel-2022/>

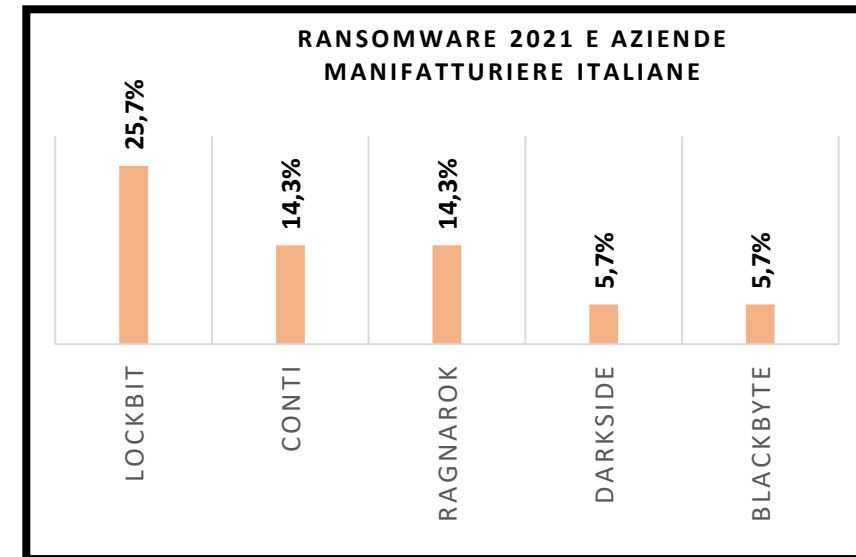
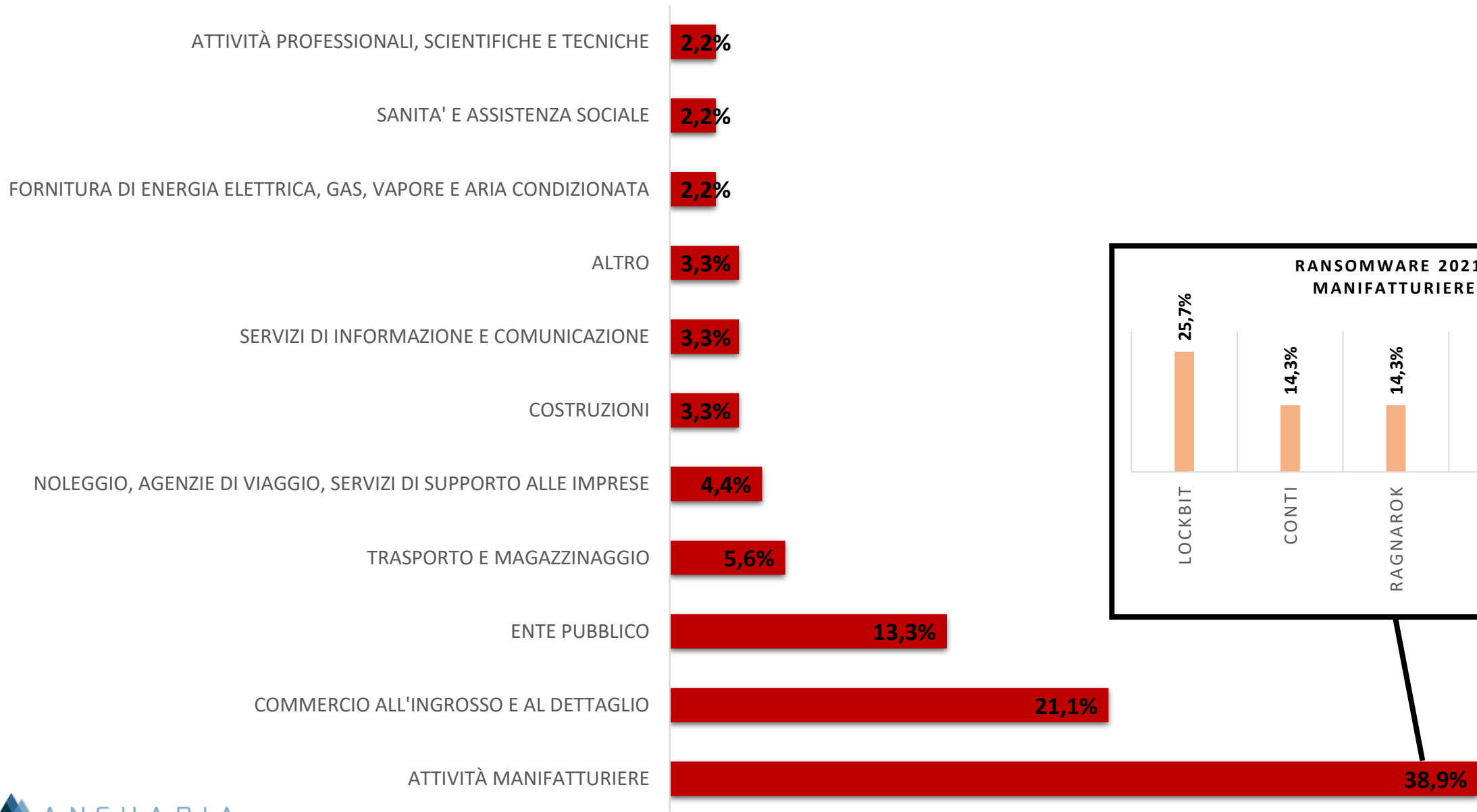
Chi sono i principali gruppi ransomware?

Nel 2021, tra i primi cinque posti, troviamo il gruppo Conti con circa il 20% degli attacchi totali, seguito da Lockbit (ora LockBit 2.0) con circa il 15%, Pysa con circa l'8%, Avaddon (che in estate ha chiuso i battenti pubblicando le chiavi per la decrittografia dei file cifrati) e Revil con circa il 7%.

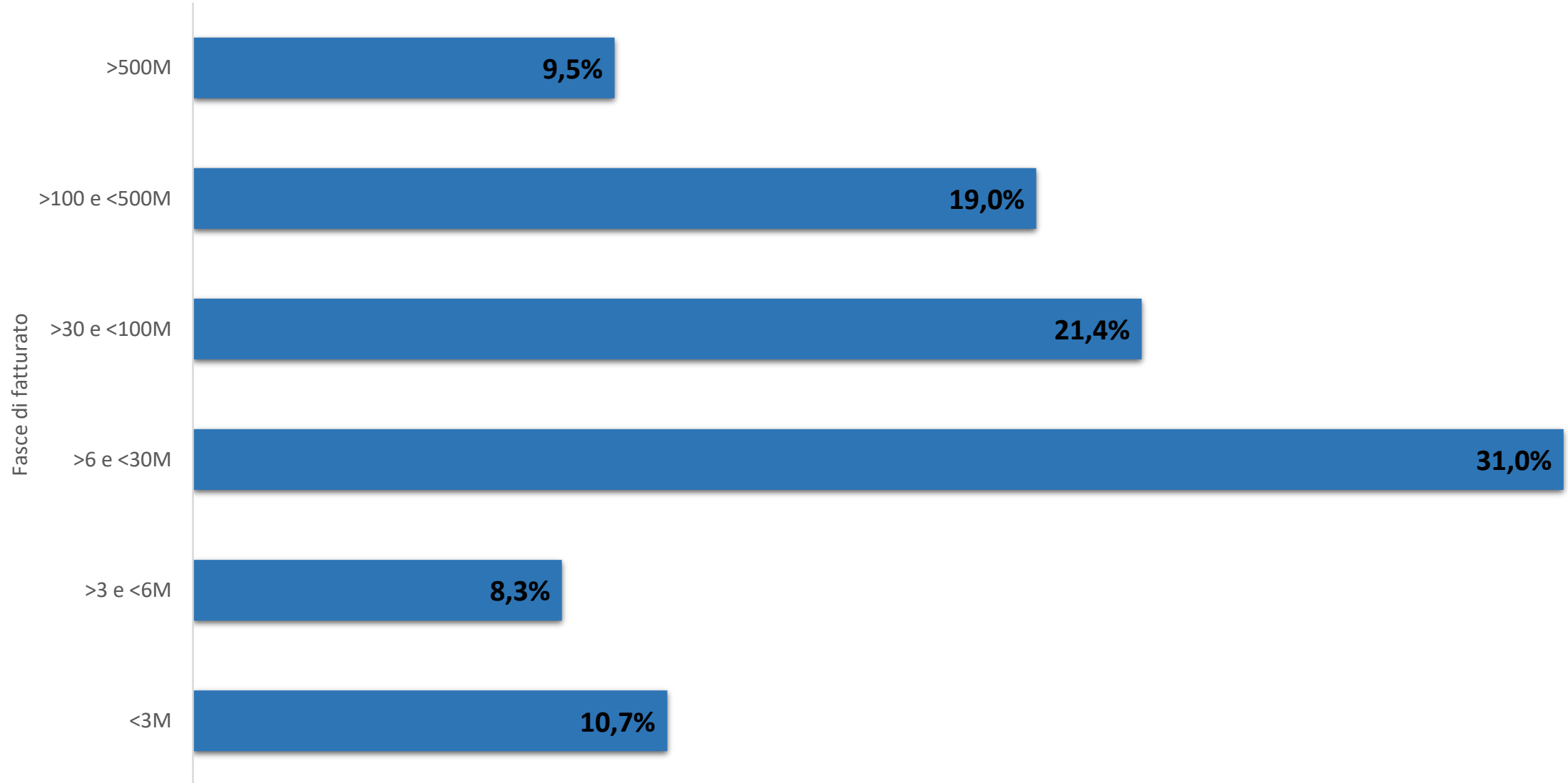


■ Conti	■ LockBit	■ Pysa	■ Avaddon
■ Sodinokibi (REvil)	■ CLOP	■ DarkSide	■ Grief
■ DoppelPaymer	■ LV	■ Hive	■ Everest
■ Prometheus	■ Babuk locker	■ AvosLocker	■ CoomingProject
■ BlackMatter	■ Spook	■ Ragnarok	■ BlackByte
■ Haron	■ Cuba	■ Vice Society	■ Payload.bin
■ RansomEXX	■ XING locker	■ Lorenz	■ NetWalker
■ Nefilim	■ Astro Team	■ Moses Staff	■ Ragnar_Locker
■ El_Cometa (SynACK)	■ Mount Locker	■ Groove	■ Lockdata
■ Bonaci Group	■ Suncrypt	■ Hotarus	■ Karma

Quali sono i settori maggiormente colpiti in Italia?

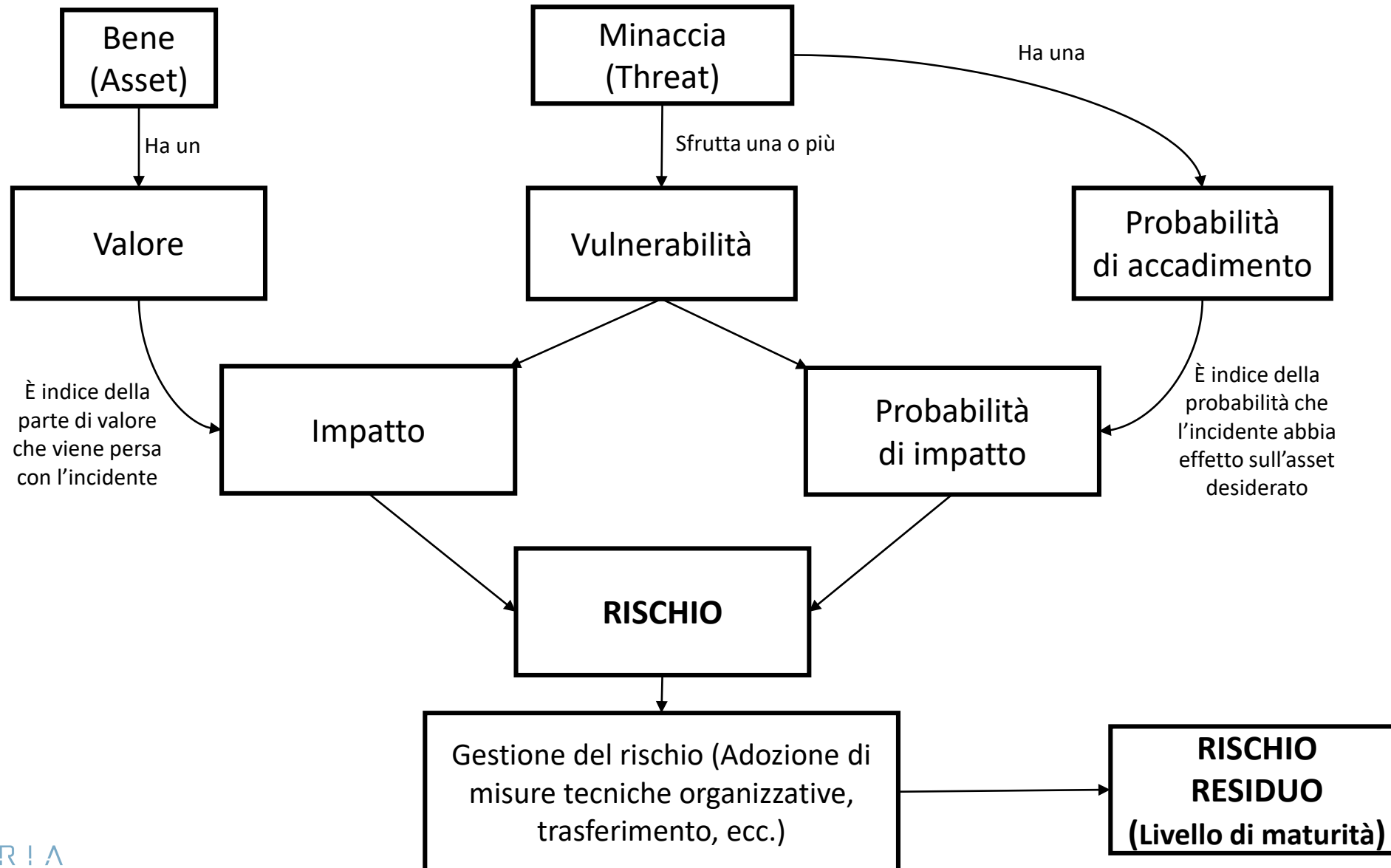


Ransomware e fatturato società italiane



Prevenire è meglio che curare

Come prevenire un attacco ransomware



Come rispondere ad un attacco ransomware

