UNIVERSITÀ DEGLI STUDI DI UDINE

LE FRONTIERE DELLA CYBER-RESILIENZA: NUOVI PARADIGMI TRA “SAFETY” E “SECURITY”

Prof. Marino Miculan
DMIF, Università degli Studi di Udine

13 maggio 2024

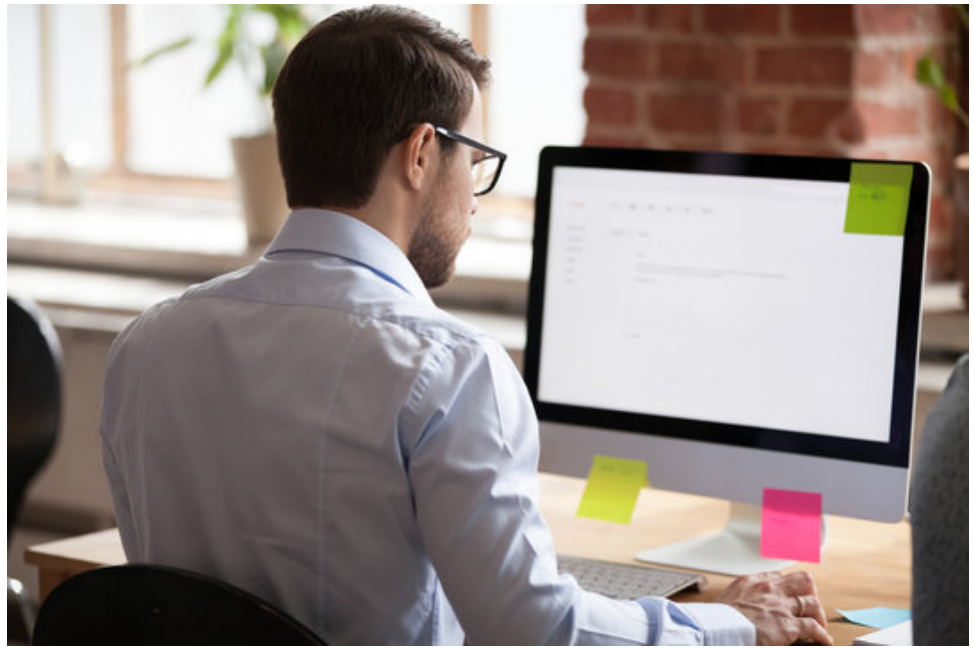
GLI OBIETTIVI DELLA SICUREZZA INFORMATICA

La sicurezza informatica ha come obiettivi:

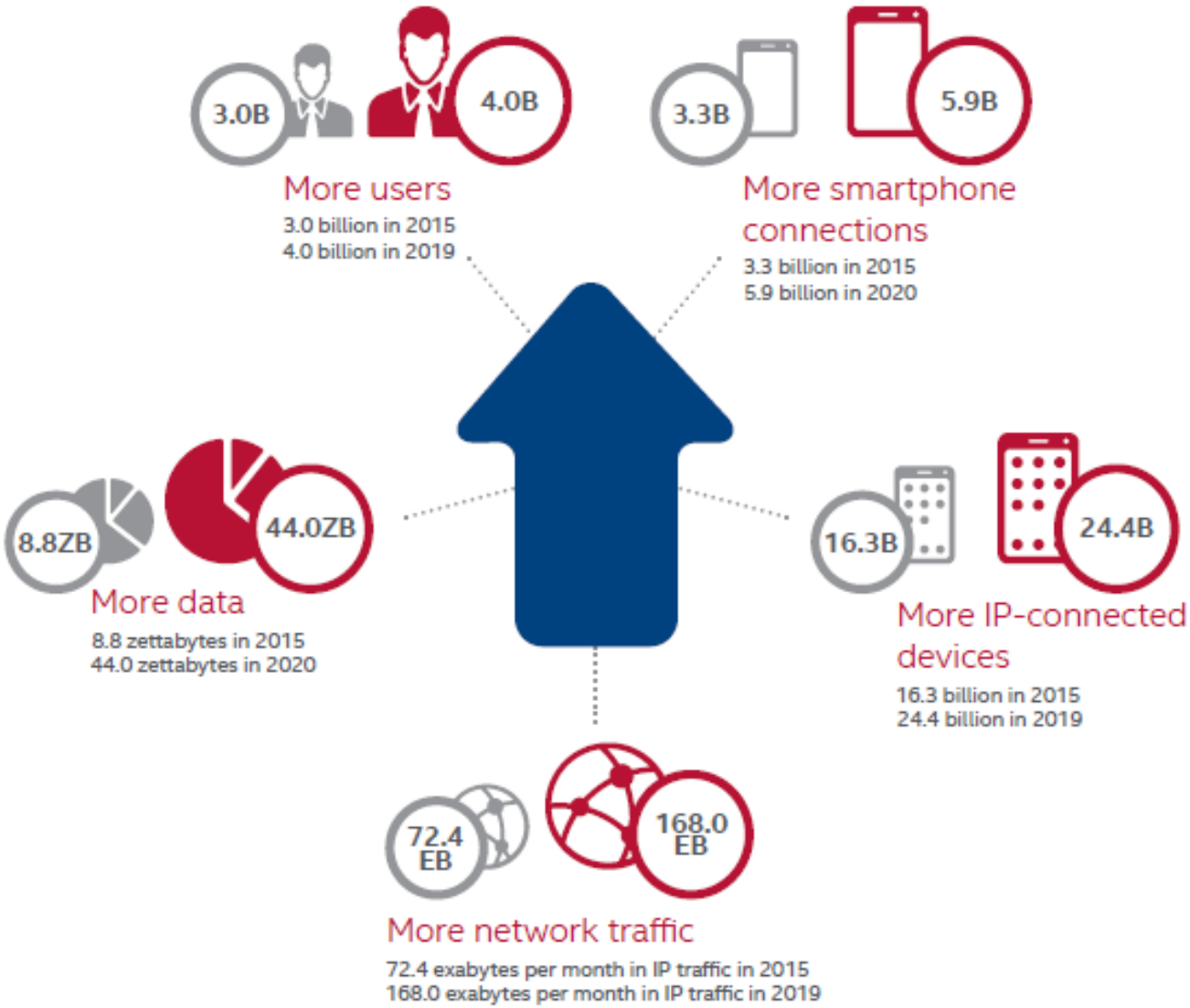
- il controllo dell'accesso alle risorse (**riservatezza**)
- la protezione delle risorse da danneggiamenti volontari o involontari (**integrità**)
- la **disponibilità** delle risorse a chi ne ha diritto nel momento in cui deve accedervi

Quali sono le risorse oggetto della sicurezza informatica

- … nell'Information Technology
  - I dati, sia memorizzati su dispositivi, sia in transito sulle reti
  - Le risorse computazionali (CPU, memoria, spazio disco, ecc)



Maggiore la digitalizzazione, maggiore la superficie d'attacco

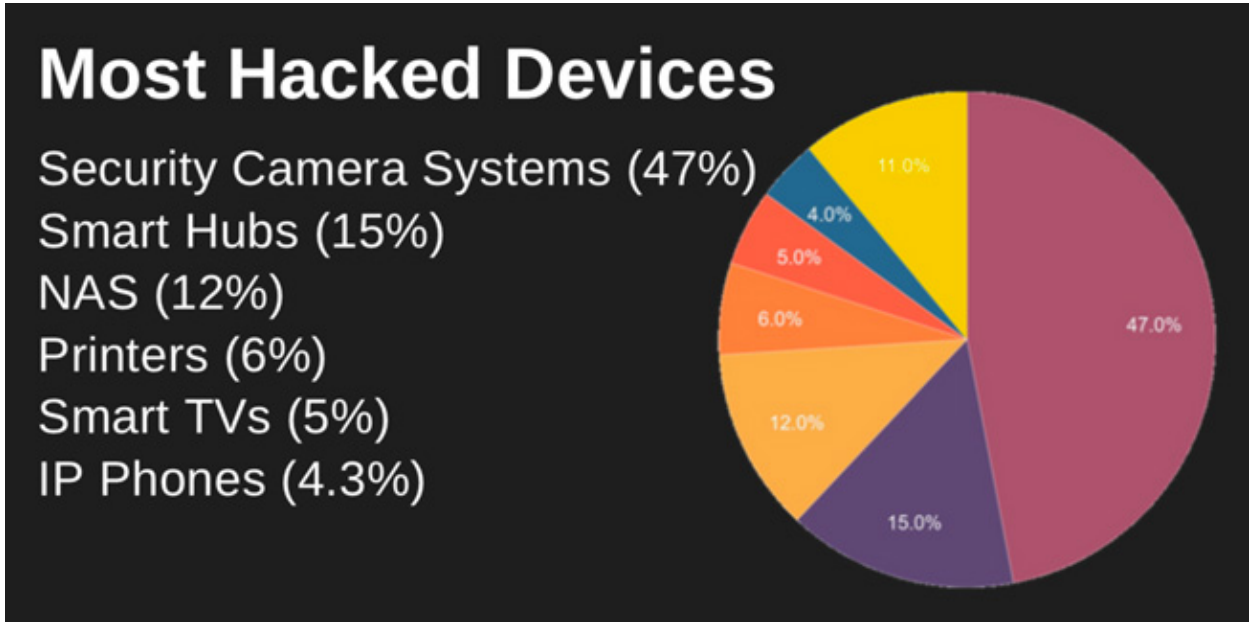


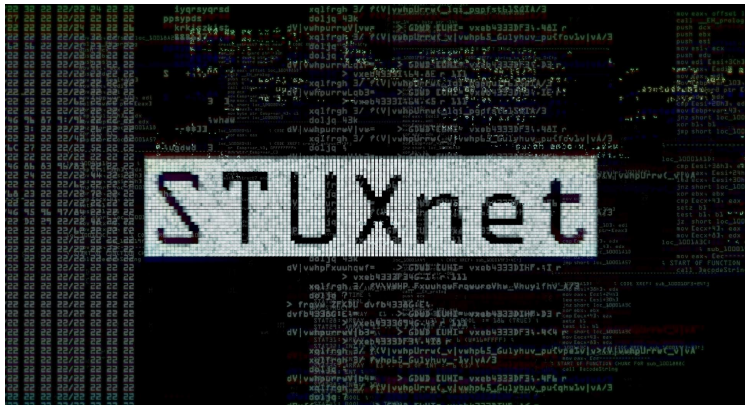
La sicurezza non è più opzionale

- Il **Codice dell'Amministrazione Digitale** spinge verso il **progressivo abbandono della carta** a favore delle **tecnologie digitali**, le quali **richiedono adeguate misure di sicurezza**
- Il **GDPR**:
  - impone una forte tutela dei dati personali
  - obbliga ad adottare **rigorose ed adeguate misure di sicurezza**
  - prevede severe sanzioni
- La **Direttiva NIS2** e il **Perimetro nazionale**:
  - impongono la protezione dei propri servizi mediante adeguate misure di sicurezza
  - impongono obbligo di **autovigilanza e denuncia** degli incidenti significativi
  - prevedono severe sanzioni

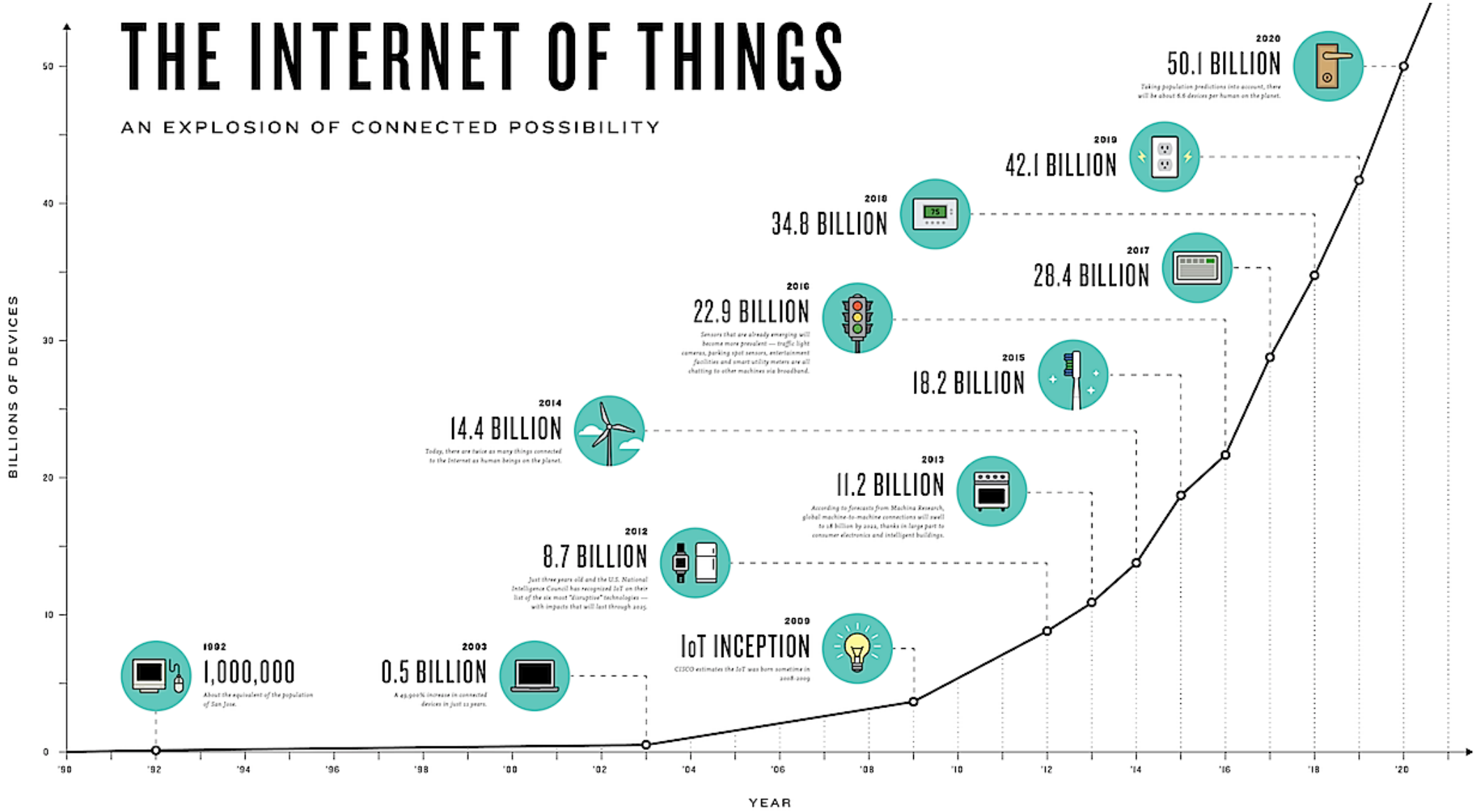
Quali sono le risorse oggetto della sicurezza informatica

- … nell'Operational Technology
  - Come sopra, ma gli obiettivi possono essere anche i **processi fisici** controllati dai sistemi informatici
  - IoT, Industria 4.0, e-Health ecc.





L'Internet delle cose e i nuovi rischi



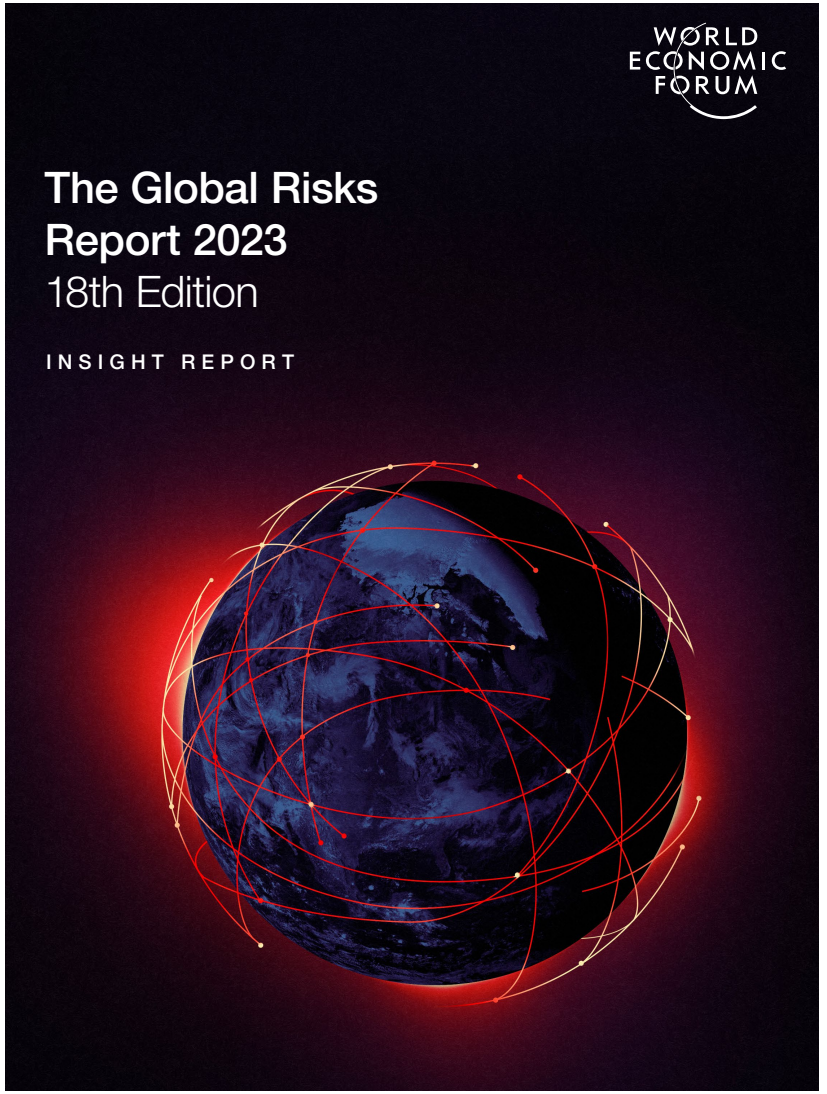
Quali sono le risorse oggetto della sicurezza informatica

- … nella *Socionology* (cit. Paul Hunter Strategy and Leadership group)
  - Il confine tra norme sociali e capacità tecnologiche sta scomparendo
  - Cambiamenti sociali sono causati dall'avvento di tecnologie, o da atti che avvengono su piattaforme tecnologiche
  - Gli attaccanti possono mirare ad avere un impatto su una società (p.e. modificare elezioni) attraverso strumenti tecnologici

Cambridge Analytica

World Economic Forum "The Global Risks Report"

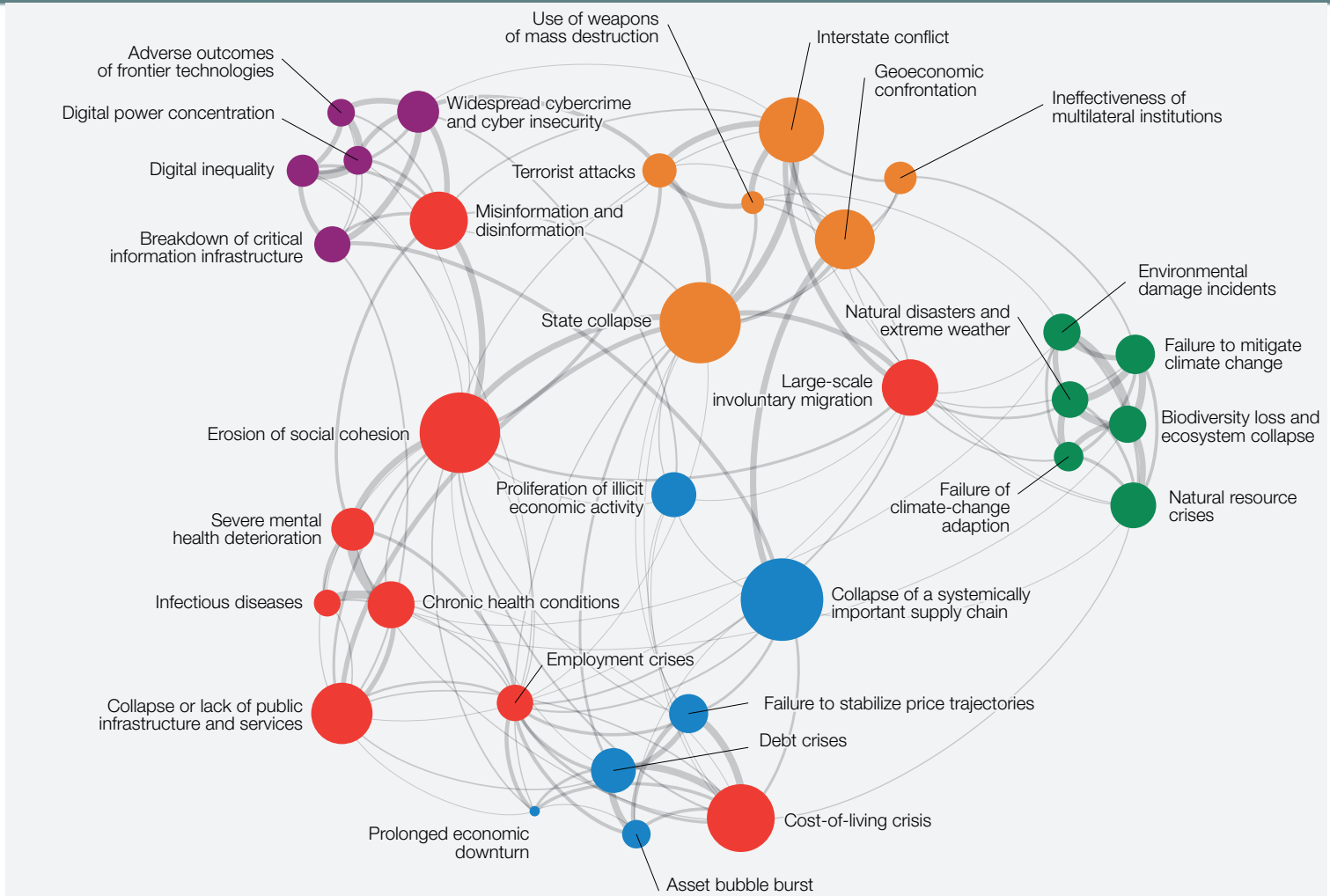
- La situazione è **peggiorata** negli ultimi anni
- "The COVID-19-induced shift to remote work has accelerated the adoption of platforms and devices that allow **sensitive data** to be shared with third parties—cloud service providers, data aggregators, application programming interfaces (APIs) and other technology-related intermediaries. These systems, while powerful tools for data and processing, attach an **additional layer of dependency on service providers**."
- "growing cyberthreats are outpacing societies' ability to effectively prevent and manage them."
- (Source: WEF Global Risk Report 2022)



Global risks landscape: an interconnections map

"Il sempre crescente intreccio delle tecnologie con il funzionamento delle società sta **esponendo le popolazioni a minacce interne dirette**, comprese quelle che cercano di distruggere il funzionamento della società. Parallelamente all'aumento della **criminalità informatica, i tentativi di interrompere le risorse e i servizi tecnologici critici diventeranno più comuni**, con attacchi previsti contro l'agricoltura e l'acqua, i sistemi finanziari, la **sicurezza pubblica**, i **trasporti**, **l'energia e le infrastrutture di comunicazione domestiche**, spaziali e **sottomarine**."

(Source: WEF, Global Risks Report 2023)

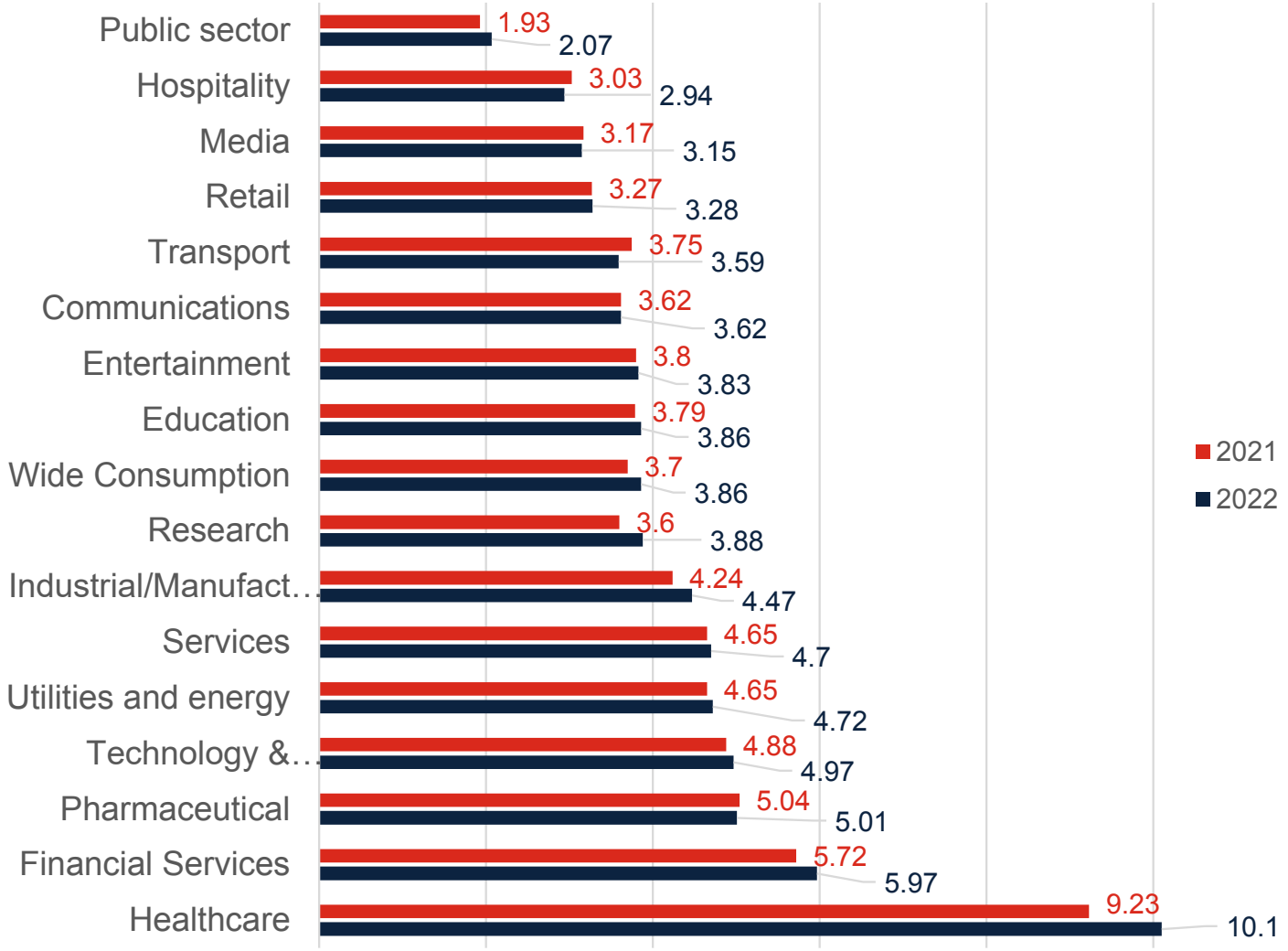


Source

World Economic Forum, Global Risks Perception Survey 2022-2023.

Il rischio informatico è in crescita nel panorama globale

- Costo medio annualizzato del CyberCrime per settore industriale (in Mln USD)
- (source: Ponemon Cost of a Data Breach Report 2022)



Il rischio informatico è in crescita nel panorama globale

Risk categories

- Economic
- Environmental
- Geopolitical
- Societal
- Technological

2 years

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

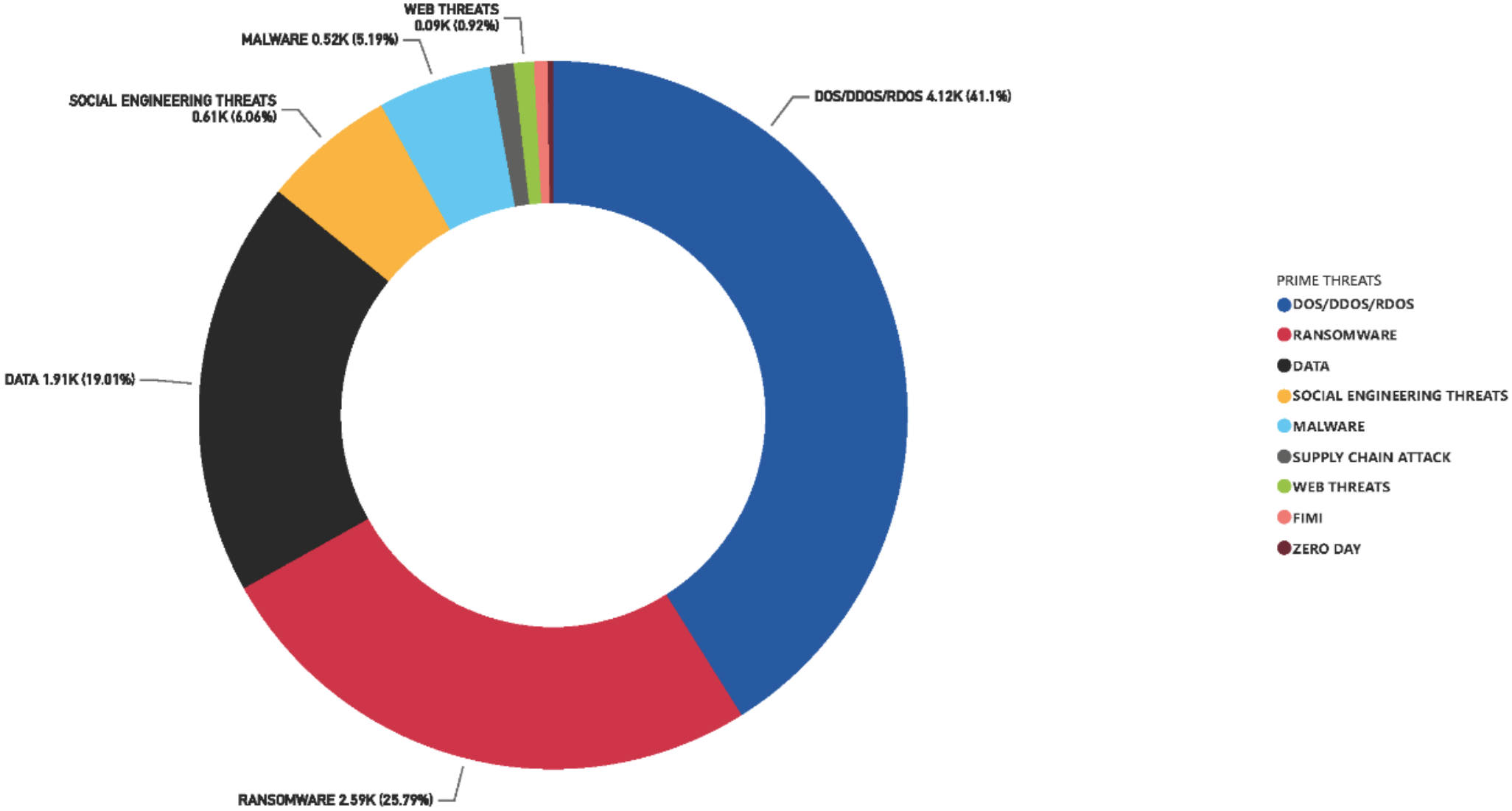
10 years

1st	Extreme weather events
2nd	Critical change to Earth systems
3rd	Biodiversity loss and ecosystem collapse
4th	Natural resource shortages
5th	Misinformation and disinformation
6th	Adverse outcomes of AI technologies
7th	Involuntary migration
8th	Cyber insecurity
9th	Societal polarization
10th	Pollution

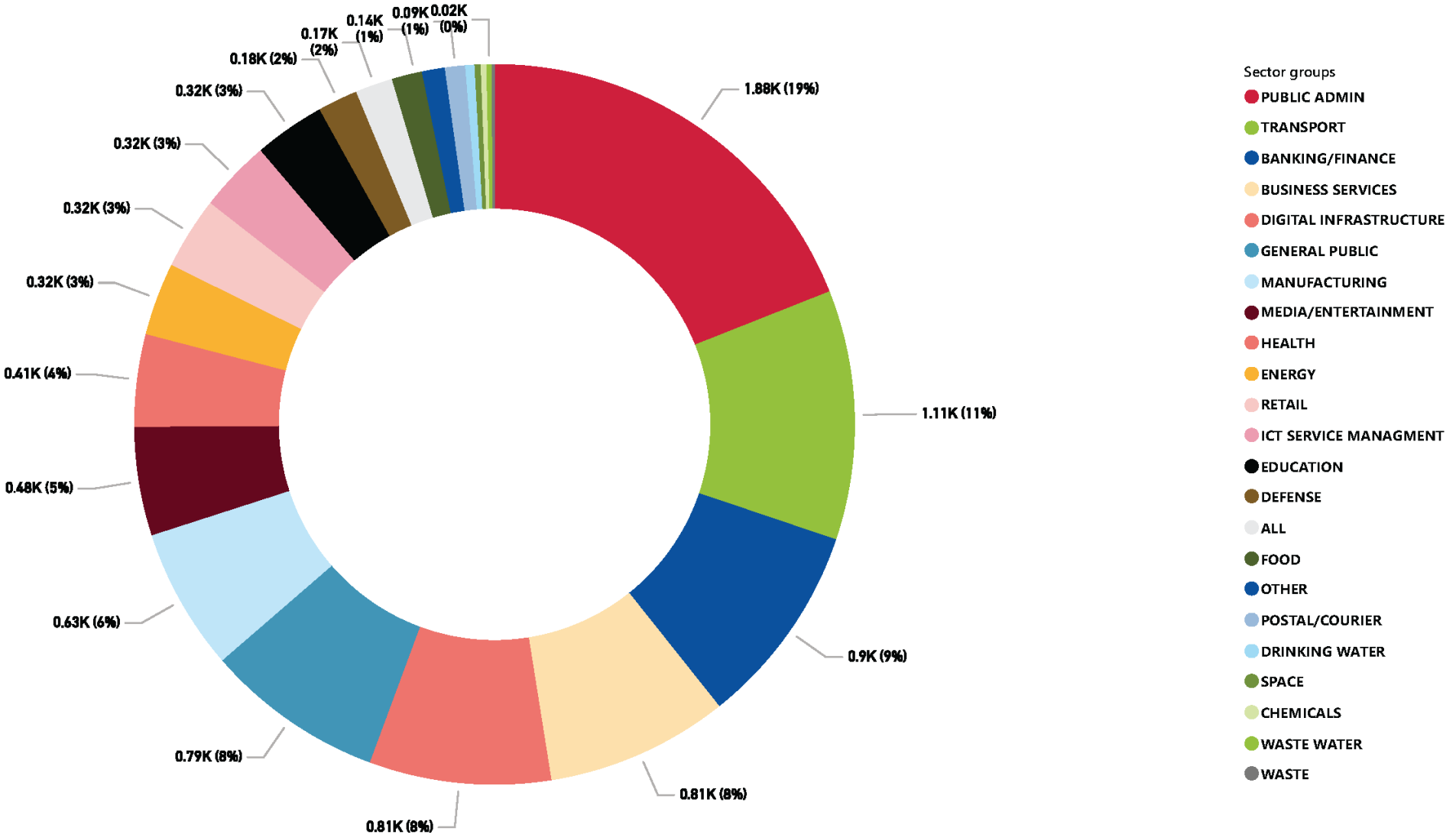
Source

World Economic Forum Global Risks Perception Survey 2023-2024.

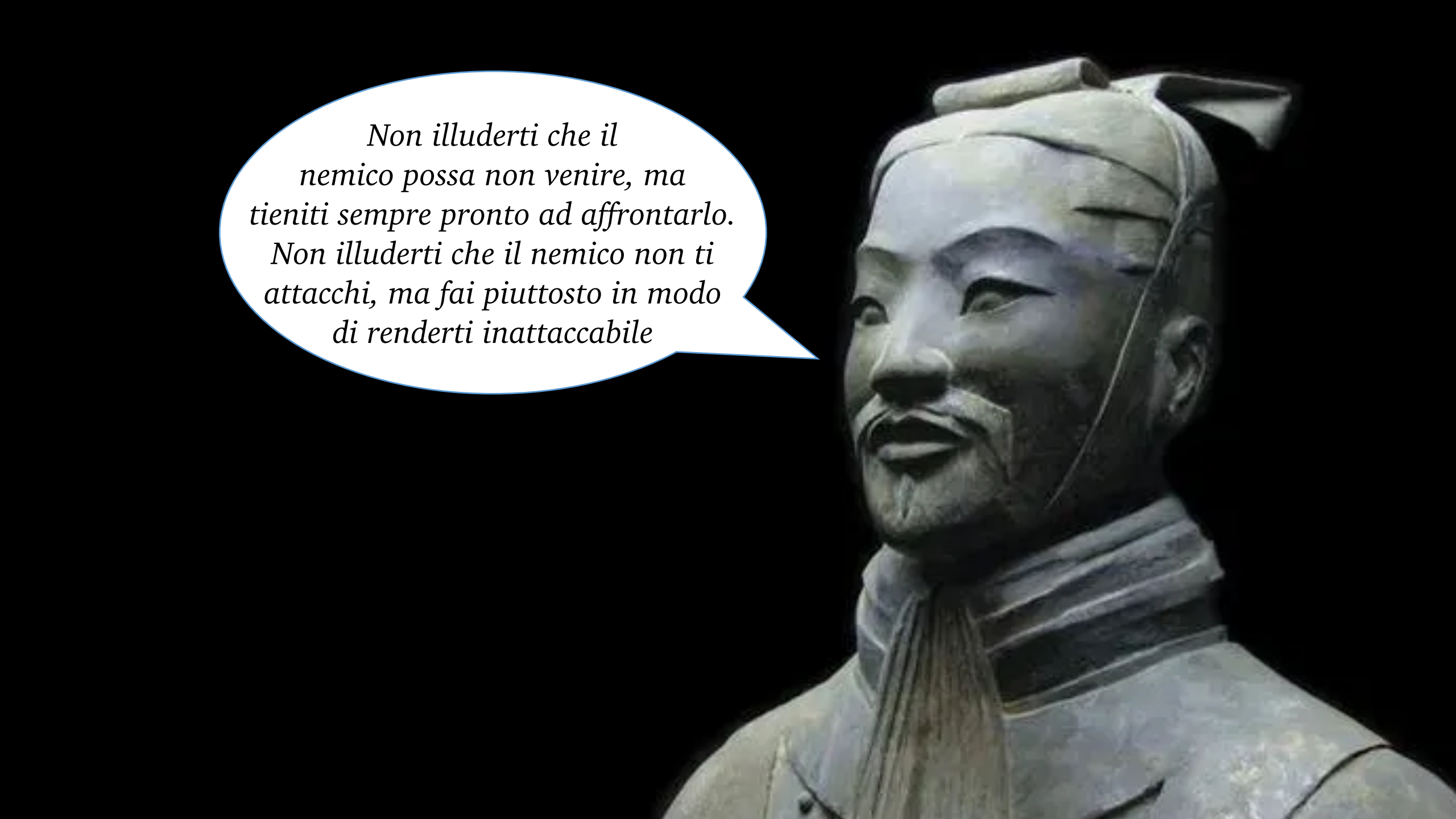
WHAT: GRUPPO DI MINACCE - LUGLIO 2023-GIUGNO 2024



WHAT: SETTORI INTERESSATI - LUGLIO 2023-GIUGNO 2024



Ma allora, come possiamo aumentare la resistenza agli attacchi informatici?


Non illuderti che il nemico possa non venire, ma tieniti sempre pronto ad affrontarlo. Non illuderti che il nemico non ti attacchi, ma fai piuttosto in modo di renderti inattaccabile

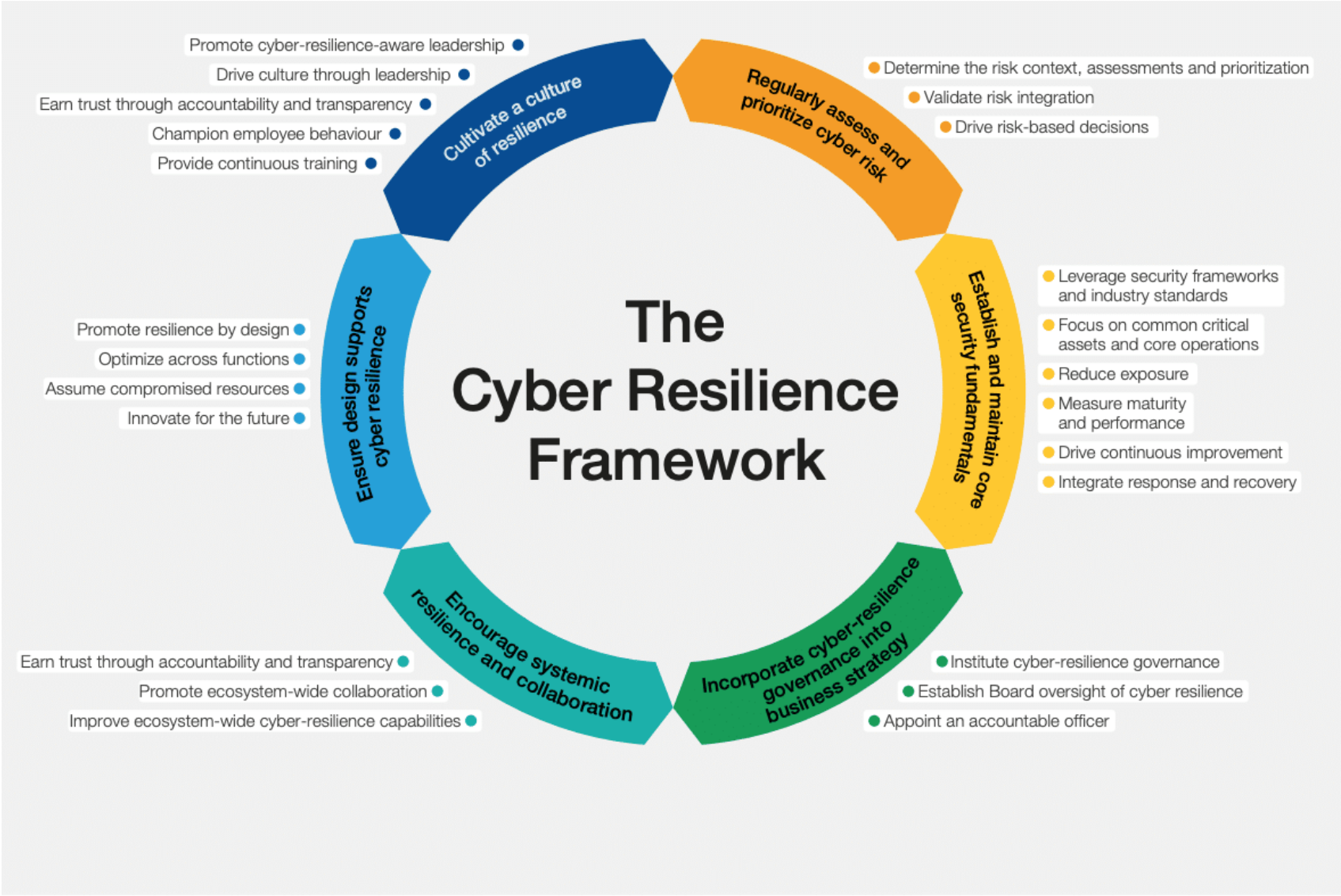
COME SI IMPLEMENTA LA SICUREZZA INFORMATICA?

- **La sicurezza informatica è un processo, non un prodotto**
- Per creare sicurezza bisogna studiare:
  - chi può attaccare il sistema, perché lo fa e cosa cerca;
  - quali sono i punti deboli del sistema;
  - quanto costa la sicurezza rispetto al valore da proteggere e rispetto al valore dei danni causati
  - Come rilevare gli attacchi al sistema
  - Come rispondere e rimediare agli attacchi
- Serve personale specializzato per queste attività

Cyber Resilience Framework

- Il CRF è una guida alle migliori pratiche per costruire una resilienza informatica in un'organizzazione.
- Si compone di sei principi chiave, pratiche associate e relative sotto-pratiche, grazie ai quali i responsabili della sicurezza informatica possono definire chiaramente una robusta resilienza informatica organizzativa.
- Costituisce un framework standard, indipendente dal settore, con risultati definiti che può fungere da base di riferimento per tutte le organizzazioni

COME SI IMPLEMENTA LA CYBER RESILIENZA?



Source: World Economic Forum and Accenture

I 6 principi del Cyber Resilience framework

1. **Valutare e stabilire le priorità regolarmente per il rischio informatico**: la gestione della cyber-resilienza è guidata direttamente dal rischio.
2. **Definire e mantenere i principi fondamentali della sicurezza**: le funzioni principali della mission aziendale e i sistemi di supporto sono sicuri di fronte ad attacchi imprevisti.
3. **Integrare la governance della cyber-resilienza nella strategia aziendale**: la cyber-resilienza è gestita in tutta l'organizzazione, dall'alto verso il basso, secondo una strategia coesa e allineata agli obiettivi aziendali.

- (Continua)

I 6 principi del Cyber Resilience framework

4. **Incoraggiare la resilienza e la collaborazione sistemiche**: l'organizzazione comprende le interdipendenze all'interno del proprio ecosistema, interagisce con le altre organizzazioni e svolge il proprio ruolo nel mantenimento della resilienza dell'ecosistema.
5. **Garantire che il design supporti la cyber-resilienza**: agilità e adattabilità sono parte integrante della strategia, della progettazione e dell'esecuzione della cyber-resilienza dell'organizzazione, che migliorano costantemente per ottimizzare la resilienza.
6. **Coltivare una cultura della resilienza**: i dipendenti sono incoraggiati a comprendere e ad adottare comportamenti di cyber-resilienza.

Conclusioni - 1

- Minacce principali: **DDoS, ransomware, ingegneria sociale, minacce legate ai dati, manipolazione delle informazioni, catena di fornitura** e **malware**.
- Notevole aumento degli **attori "professionisti"** che offrono programmi di attacco as-a-Service, impiegando nuove tattiche e metodi alternativi per infiltrarsi negli ambienti.
- Settori più colpiti: **pubblica amministrazione** (~19%), seguito da specifici soggetti (~11%), dalla **sanità** (~8%), dalle **infrastrutture digitali** (~7%) e dal **settore manifatturiero, finanziario e dei trasporti**.

Conclusioni - 2

- **La cyber-sicurezza non è un prodotto**
- La sicurezza è una **cultura aziendale**
  - va maturata con un'adeguata educazione
- La sicurezza è un **processo globale**
  - impatto trasversale sulle attività dell'organizzazione
- La sicurezza è un **servizio specializzato**
  - Richiede l'istituzione di apposite strutture
- La sicurezza richiede **risorse da gestire**
  - complesso mix di competenze, risorse, prodotti